INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

DOCUMENTO DE PRESERVACIÓN DIGITAL EN INTERNET ARCHIVE

Vol. 4 Núm. 1 (2020): Enero-Junio

1. **Estudio de factibilidad de un sistema de bajo costo para la monitorización del tráfico de vehículos por medio de la detección de dispositivos WiFi**
2. **La importancia de la autenticación multifactor para el usuario final en un entorno financiero.**
3. **Estudio exploratorio de la seguridad del DNI electrónico para su aplicación en Ecuador**
4. **Usabilidad de herramientas HCI que mejoran la capacitación en la gestión de emergencias**
5. **APLICACIÓN DE LAS TIC EN LA ENSEÑANZA DEL ELECTROMAGNETISMO PARA CARRERAS DE INGENIERÍA**
6. **Aplicación de Realidad Virtual en el tratamiento de acrofobia en personas que practican deportes extremos como el paracaidismo**

Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0)

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 1-12 ISSN 2550-6730

Recibido: 14/02/2020
Aceptado: 15/04/2020

Aplicación de Realidad Virtual en el tratamiento de acrofobia en personas que practican deportes extremos como el paracaidismo.

Navas Moya-Germánico [1] Mayorga Soria-Paulina [2] Mayorga Soria-Paúl [3] Navas Moya-Milton [2]

[1]Academia de Guerra, Quito, Ecuador,
[2]Universidad de las Fuerzas Armadas ESPE, Sangolqui, Ecuador,
[3]Dirección de la Industria Aeronáutica,
gjnavasm@ejercito.mil.ec, ptmayorga@espe.edu.ec, paulmayorgafae@gmail.com, mpnavas@espe.edu.ec

RESUMEN
En la actualidad cualquier actividad que realice el ser humano puede estar relacionado con el miedo patológico, la acrofobia a través de los años ha sido uno de los miedos irracionales presentes en las personas, produciendo grandes consecuencias en la vida diaria no solo por el hecho de estar presente en un entorno que implique altura, sino también con la situación de imaginarse, esto puede ocasionar en la persona síntomas como la ansiedad, sudoración y temor. En el presente documento se trata el paracaidismo y el tratamiento de la acrofobia mediante la realidad virtual. Además, una alternativa de implementar la aplicación mediante herramientas de desarrollo y de realidad virtual en sus versiones de prueba y código abierto. Se presenta los resultados obtenidos mediante la validación a las sesiones terapéuticas realizadas a personas que practican este deporte, donde se obtiene la reducción de estrés emocional o cognitivo funcionando de manera sólida y estable, la eficiencia de la aplicación de realidad virtual se sustenta en pruebas unitarias sucesivas en personas que son aspirantes al curso de especialización de Paracaidismo.
Palabras-clave: acrofobia; realidad virtual; programación; paracaidismo; ambientes.

ABSTRACT
Nowadays any activity that the human being carries out can be related to the pathological fear, acrophobia through the years has been one of the irrational fears present in people, producing great consequences in the daily life not only for the fact of being present in an environment that implies height, but also with the situation of imagining, this can cause in the person symptoms like anxiety, sweating and fear. In this document, skydiving and the treatment of acrophobia using virtual reality are discussed. In addition, an alternative to implement the application through development tools and virtual reality in its trial and open source versions. The results obtained through the validation of therapeutic sessions carried out with people who practice this sport are presented, where the reduction of emotional or cognitive stress is obtained, working in a solid and stable way. The efficiency of the application of virtual reality is supported by successive unit tests on people who are candidates for the Parachuting Specialization Course.
KEYWORDS: phobia; virtual reality; programming; parachuting; environments.

1. Introducción

Actualmente en el mundo los trastornos mentales desempeñan un papel importante en la salud. Esto se debe a que un gran número de personas sufren de tales disturbios. De acuerdo con la Organización Mundial de la Salud[1], un gran número de personas en todo el mundo sufren algún tipo de trastorno psicológico[2]. Las fobias forman parte de los trastornos mentales y se clasifican como un subtipo del trastorno de ansiedad que en ocasiones conllevan problemas graves en su estado de salud[3]. Se define la fobia como un miedo persistente e incontrolable de un objeto, persona, animal o situación. Puede causar reacciones fisiológicas como falta de aire, mareo, taquicardia, temblores, sudores, entre otros[4].
En Latinoamérica se está usando la realidad virtual como una técnica que posibilita la creación y exposición de pacientes a los distintos ambientes virtuales muy similares a lo real[5][6]. De acuerdo a la Organización Panamericana de la Salud (OPS) el paciente recibe estímulos virtuales equivalentes a los reales, causando así la ansiedad necesaria para el tratamiento. Diversos estudios describen la utilización de la realidad virtual en diferentes fobias como: la acrofobia[7] y la fobia a saltar de un avión ya sea por caída libre o paracaidismo[8]. Se propone una solución utilizando simuladores durante el tratamiento sin necesidad de recurrir al mundo real, usando las gafas de realidad virtual de cualquier tipo, escenarios variados que introducen a diferentes niveles de ansiedad[9][7].
Ecuador a través del Instituto Politécnico Nacional de México adoptó el SASUFO (Sistema Inmersivo Terapéutico), el cual se encarga de recrear varios escenarios de realidad virtual en donde el paciente vive su miedo, pero de forma controlada. En el caso de la creación de escenarios, estos se hicieron con base en la opinión de los especialistas para que la exposición al temor fuera progresiva. La creadora explicó: El visor Oculus Rift permite al paciente que simule lo alto de un rascacielos, y así brinda una experiencia inmersiva con lo que el usuario tiene la libertad de movimiento para voltear y caminar en el mundo virtual[10].
Mediante esta nueva tecnología se pretende disminuir la acrofobia mediante la simulación de entornos ficticios en diferentes alturas y ambientes utilizados en el paracaidismo[11]. El usuario por medio de terapias con esta aplicación podrá asimilar el ambiente en la vida real así disminuyendo las consecuencias que provoca esta fobia[12][10].
La aplicación presenta escenarios virtuales diseñados para ayudar a superar la fobia a las alturas, presentándoles pruebas que ayuden a enfrentar los temores, mediante la flexibilidad en ejercicios, mover cada día el tiempo de exposición a las alturas tratando de no acrecentar los recelos a realizar el deporte extremo del paracaidismo. Las perspectivas cognitivas de las fobias son estímulos muy importantes ante la aplicación de la Realidad Virtual como método alternativo para poder mitigar la ansiedad y la fobia a las alturas, por lo tanto, la investigación busca ayudar a que el paciente mantenga la calma el momento de ejecutar el salto, también se cuenta con estadísticas del proceso para establecer el tiempo de duración del tratamiento.

2. Materiales y Métodos

El vertiginoso avance tecnológico que ha venido experimentando la realidad virtual últimamente ha llegado al punto de reproducir con seguridad diferentes situaciones que en la cotidianidad pueden ser peligrosas. Para tratar de mitigar estos peligros se plantea la implementación de la realidad virtual con el afán de controlar problemas como el vértigo, las fobias, los miedos, entre otros. Las personas que sufren del trastorno de acrofobia pueden experimentar miedo a grandes alturas, tienen altas probabilidades de sufrir accidentes, la tecnología de realidad virtual ayuda a estas personas a que venzan sus miedos y tengan un entorno seguro y controlado.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 1-12 ISSN 2550-6730

2.1. Paracaidismo

El paracaidismo es un deporte o una técnica que consiste en saltar desde grandes alturas o desde un avión, en el cual el deportista o los participantes regresan a tierra[13][14], en algunos lugares es considerado como una actividad de alto riesgo, por lo que se debe tomar en cuenta muchas seguridades[15], siendo esta una actividad extrema y que el aterrizaje conlleva un impacto que genera temor entre las personas que realizan esta actividad[16], para garantizar esta acción se debe precautelar y supervisar las actividades como verificar el equipo, cuidar que la cúpula se abra automáticamente[17].

2.2. Acrofobia

La acrofobia se le denomina al miedo intenso por las alturas, misma que causa ansiedad y pánico significativo[18], son muchas las personas que experimentan incomodidad o angustia cuando se exponen a las alturas, pero estos trastornos no tienen que ser necesariamente acrofobia[7]. Debido al miedo a las alturas las personas con este problema tienden a tener mareos, por lo que evitan cualquier posibilidad de situaciones que tengan que ver con situaciones de mayor altitud[12].

2.3. Realidad Virtual

Es una tecnología que permite la creación de espacios tridimensionales por medio de un computador esto quiere decir que permite la simulación de la realidad, con la gran ventaja de que podemos introducir en el ambiente virtual los objetos y crear los acontecimientos que se consideren útiles, según el objetivo planteado[19]. La realidad virtual nos ayuda a experimentar cosas a través del computador que realmente no existen, transportándonos a mundos virtuales logrando experimentar lugares o momentos mediante tecnologías inmersivas que coadyuvan a que el cerebro almacene ubicaciones y lugares donde físicamente no está el paciente.[20][21]

2.4. Visual Studio

Es un paquete de desarrollo el cual integra una amplia gama de lenguajes de programación y librerías las mismas que ayudan a facilitar a los desarrolladores en sus actividades, con diversas características que se pueden usar para muchos aspectos de software, como por ejemplo editar, depurar y compilar código y, después, publicar distintas aplicaciones sean de escritorio, web y móviles.[22].

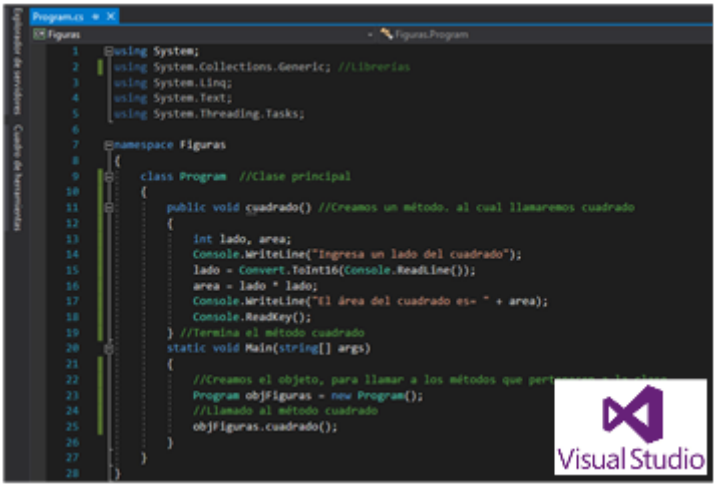

Figura 1: Diseño de la aplicación en Visual Studio

2.5. Blender

Es una suite de creación de ambientes 3D de código abierto y gratuito que se ejecuta en multiplataformas, generalmente utilizado para crear objetos 3D como imágenes fijas, animaciones, tomas VFX y edición de video, ofrece una amplia gama de herramientas esenciales, que incluyen modelado, renderizado, animación, edición de video, composición, texturizado, Rigging y muchos tipos de simulaciones[23]. Por la naturaleza de código abierto de este software permite añadir nuevas alternativas como las que ya se trabajan en vistas de ojo de pez que son necesarias para el domo hemisférico pantallas envolventes[24][25].

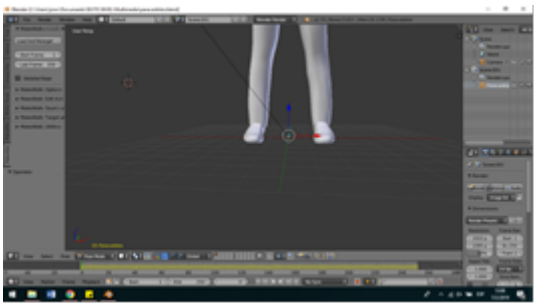

Figura 2: Diseño de la aplicación en Blender

2.6. Unity3D

Es una herramienta para desarrollo de videojuegos, está compuesto de gráficos, multimedia, inteligencia artificial, tiene propiedades multisensoriales, etc. en donde es posible crear y simular un entorno virtual[23]. Unity para realizar prácticas de realidad virtual tiene la capacidad de complementarse con otros paquetes como Blender, 3ds Max, herramientas de adobe, entre otras. Otras de las propiedades de este paquete es la tienda virtual en donde se puede buscar complementos o plugs que ayudan al desarrollo de las actividades[24][25].

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 1-12 ISSN 2550-6730

Figura 3: Ambientación del entorno en Unity

3. Desarrollo

Para la aplicación del tratamiento alternativo de la acrofobia fue diseñado en unity 3D, todo el ambiente virtual buscando asemejarse con el entorno natural para tener vivencias similares a las originales, además que se complementó la programación con el Visual Studio, que permite programar los objetos, escenas y assets de la aplicación, para el diseño 3D personalizados se utilizó el Blender, con la utilización de estas herramientas se inicia el desarrollo de un aplicativo que este en capacidad de disminuir la fobia a las alturas(acrofobia) mediante la inmersión en los entornos virtuales.

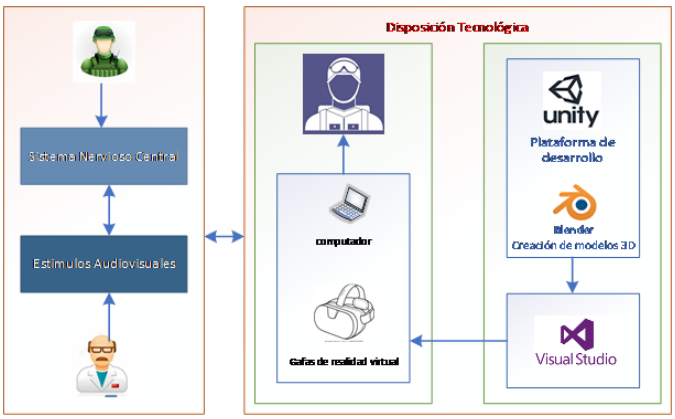

Figura 4: Diagrama de bloques de tratamiento de la fobia

El tratamiento a las fobias en la actualidad se lo desarrolla mediante la utilización de equipos alternativos a los tradicionales teniendo con claridad que es lo que se va a realizar para poder medir, esto permitió planificar de mejor manera la investigación. La mayoría de los resultados son cuantitativos ya que la tecnología permite desarrollar pruebas por un número mayor de veces sin que esto descarte la parte cualitativa que mejora los procesos de evaluación y la toma de datos. El estudio está desarrollado como una aplicación virtual en unity 3D, contiene scripts de control, los mismos que actúan de acuerdo con el comportamiento de los dispositivos aplicados en el entorno Unity.

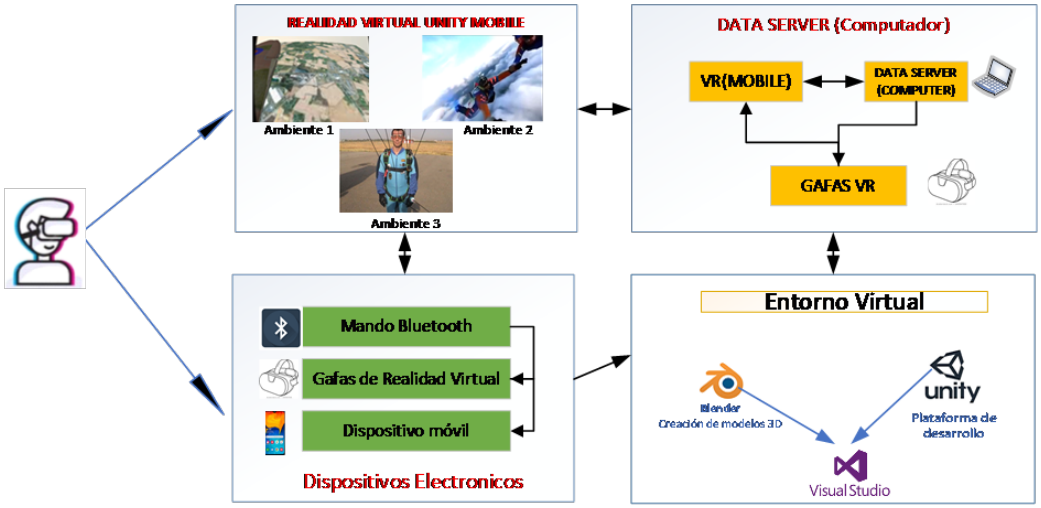

Figura 5: Esquema funcional de trabajo

En el esquema se puede observar el flujo y los componentes que intervinieron en la aplicación de la investigación partiendo de la persona (usuario), y todos los componentes tanto de hardware y software en donde se muestra como está estructurado el sistema en sus diferentes fases, scripts, etc. El usuario tiene la oportunidad de intervenir en la etapa de simulación de la escena mediante la realidad virtual la misma que está dividida en ambientes que ayudaran a la superación del problema del usuario, en el Data Server se desarrolló las animaciones mediante la utilización de un computador, se diseñó una app móvil la que será incluida en un celular y este a su vez en unas gafas de realidad virtual. En el entorno virtual se muestra las herramientas que se utilizaron para el desarrollo de este entorno, en donde se puede ver el modelado y el mezclador de las imágenes 3D, así como el texturizado. El propósito de este segmento es modelar al actor(paracaidista), el ambiente en el cual se puede ver las imágenes del cielo con sus nubes y cuando se sobrevuela ciertos paisajes.

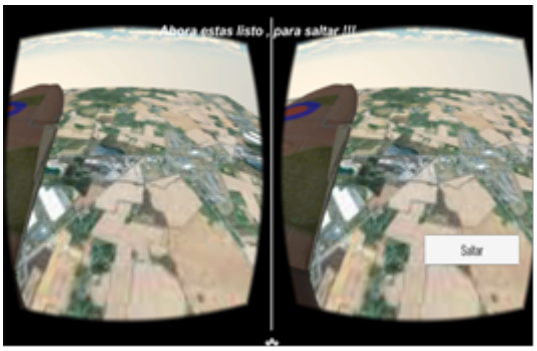

Figura 6: Entorno virtual, vista desde la altura de un avión

En la imagen anterior tenemos un ambiente virtual inmersivo con espacios imaginarios de una ciudad, vista desde un avión previa al salto por paracaídas, esta escena está considerada para la investigación como la primera fase y que debe ser evaluada para continuar o no con las siguientes fases, la sensación de la altura y cubriendo grandes aéreas con su visión produce cierto grado de temor. Para poder alcanzar el objetivo se manejó algunas alternativas de ambientes virtuales resultando algunos inaccesibles o con demasiado riesgo, por lo que se hicieron varias pruebas concluyentes a fin de establecer la propuesta planteada y resultando esta la mas cercana a la realidad.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 1-12 ISSN 2550-6730

Figura 7: Entorno virtual en el cielo luego del salto de un avión

En la imagen 7, se visualiza la segunda fase de la investigación la cual muestra una alternativa de los ambientes diseñados en el que se puede apreciar ya el salto de caída libre de un paracaidista en un entorno virtual, en esta fase el paciente experimenta el salto de una manera realista y segura, la funcionalidad radica en el poder ofrecer en un alto grado la experiencia es decir la inmersión total. En ambientes como el que se presenta los usuarios viven una realidad totalmente elaborada que permite simular un mundo real, pero en formato digital y que se visualiza en una pantalla que se encarga de reproducir sensaciones en un lugar seguro.

Figura 8: Equipo de paracaidismo en 3D

En la imagen 8, se presenta la fase 3, que consiste en visualizar el equipo mediante objetos en 3D que son utilizados para la práctica del paracaidismo como deporte o como profesión, está fase se centra en ayudar al paciente para que vaya tomando confianza como un complemento al tratamiento, se puede observar que consta el casco, altímetro, el paracaídas, mono completo (ropa apropiada), gafas, etc. Esta fase es basada en la experiencia de los paracaidistas ya que debe estar acompañada de una inducción de parte del jefe y/o maestro de salto que son las personas mas experimentadas en estas actividades.

4. Resultados

Para la evaluación se aplicó la ejecución de software de realidad virtual mediante gafas especiales destinadas para esta actividad los cuales se plasmaron en las fases o niveles del aplicativo desarrollado, se estableció en coordinación con un terapeuta llevar un registro en donde se pueda plasmar el tiempo empleado en la terapia, para enfocarse en disminuir la acrofobia. La aplicación consiste en un entorno como se lo explicó en el desarrollo de la investigación donde la persona con estos síntomas deben interactuar con el personaje que va a realizar la actividad de saltar del aeroplano.

Figura 9: Pruebas de funcionamiento

En la imagen anterior se puede observar la aplicación de las pruebas a un militar previo al curso de especialización de paracaidismo, las sensaciones entre el personal que probó esta alternativa, se pudo observar que algunos usuarios sintieron la necesidad de sacarse las gafas como muestra de desesperación o miedo antes las diferentes fases del desarrollo de la aplicación de las pruebas.

Tabla 1. Resultado a las pruebas de la aplicación
Personas que realizaron el ejercicio en la aplicación RVAcrofobia

Síntomas	Ninguno	Leve	Moderado	Severo
Ansiedad anticipatoria	2	4	3	6
Miedo y pánico	1	5	2	7
Incremento del ritmo cardíaco	3	5	5	2
Sudoración	4	9	1	0
Taquicardia	9	3	2	0
Sensación de mareo o vértigo	3	3	4	5
Dolor estomacal	1	5	5	4

Como se muestra en la figura anterior las sesiones de tratamiento para mitigar la acrofobia se realizó en una población de 15 personas de las cuales 9 fueron militares y 6 civiles. Estas personas de acuerdo a las fases planteadas en el desarrollo de la investigación, estuvieron bajo la supervisión de un profesional del área de la psicología el cual era el encargado de controlar la puntuación obtenida en la aplicación de los ambientes de realidad virtual. Con la finalidad de poder obtener datos reales y que puedan ser un aporte a la investigación se realizó de corrido las dos fases teniendo como resultado los siguiente: Fase 1.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 1-12 ISSN 2550-6730

El paciente observa un entorno a gran altura con un alto nivel de realismo. Fase 2. El paciente procede a interactuar con la aplicación, al efectuar el salto de caída libre con el mismo nivel de realismo. Fase 3. Conocimiento del equipamiento con el fin de mitigar la sensación de peligro.

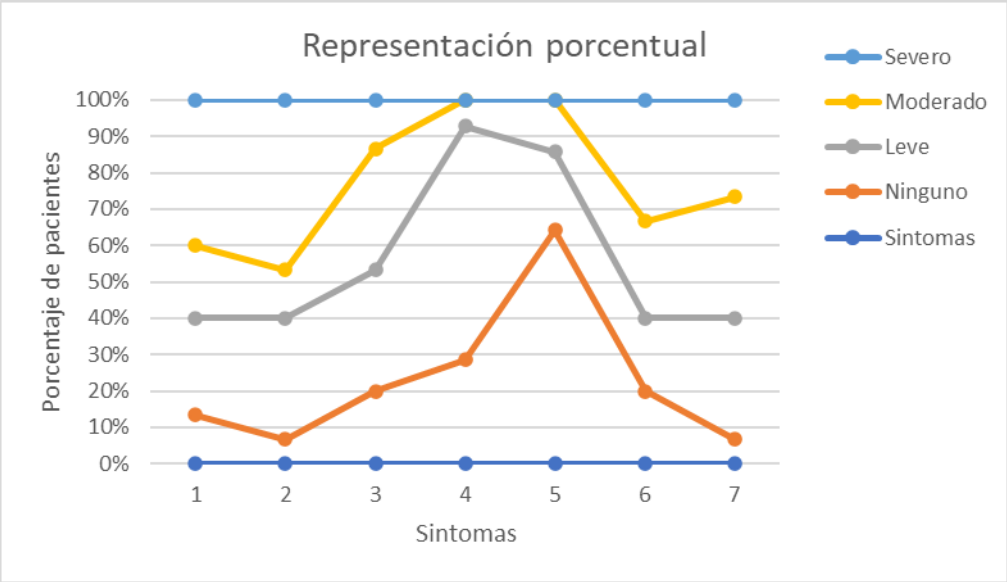

Figura 10: Representación gráfica de los resultados

La imagen 10, muestra el análisis de los indicadores de las evaluaciones con categorías sugeridas por los profesionales, concluyendo que el tratamiento mediante ambientes virtuales arrojó datos que facilitan la toma de decisiones de instructores, ya que muchos de los casos experimentan ansiedad o miedo que desborda a la hora de ejecutar la actividad. Muy pocos mostraron alteraciones en su salud como taquicardias, o incrementos en el ritmo cardiaco que sean dignos de resaltar, la sudoración se hizo presente en algunos participantes, pero en forma leve que no influye en los resultados del tratamiento, algunos manifestaron tener dolores estomacales que si fueron intensos en las pruebas que son llevaderos a la hora de realizar la actividad de paracaidismo.

5. Discusión

La realidad virtual es la alternativa hacia el aprendizaje y los tratamientos facultativos, debido a que facilitan el desenvolvimiento de pacientes con temores o alteraciones psicológicas (temores patológicos), La aplicación muestra ambientes virtuales para las personas con problemas de fobia a las alturas la misma que resultó un buen laboratorio para el personal seleccionado en la experimentación, dentro de los cuales estuvieron militares que ya tuvieron sus primeras experiencias y que tenían algún tipo de inconveniente en su formación para realizar el salto. El propósito del programa es lograr una estabilización emocional de las personas en escenarios virtuales que en lo posterior servirán para disminuir la fobia de los pacientes cuando se enfrenten a situaciones reales. Los participantes de está practica lograban “adentrarse” en el experimento al punto que en ocasiones se observaba que se incrementaban los síntomas de ansiedad, miedo, en general fobia. La contribución que hizo esta aplicación de Realidad Virtual en el campo de la psicología es muy importante ya que aporta para disminuir y controlar la fobia de los pacientes con la exposición en vivo.

6. Conclusiones

- Para desarrollar los síntomas de la acrofobia muchas veces no es necesario estar cerca de un lugar elevado o una situación que ponga en riesgo la seguridad de la persona, con solo imaginarse situaciones en las que existe un precipicio ya aparece la sensación de un intenso malestar. Se considera que la acrofobia afecta a un gran número de personas, otras al momento de la exposición muestran un gran respeto por las alturas.
- Esta aplicación que fue desarrollada según el criterio profesional de un psicólogo, puede ser aplicada en otros ámbitos educativos, didácticos y de forma especial en la salud.
- Las personas que realizaron las sesiones como parte de la terapia a través de la aplicación, se adaptaron al entorno y lograron disminuir el grado de acrofobia encontrada., con esta aplicación se contribuye a una mejor práctica del paracaidismo reduciendo el miedo a las alturas con la simulación de escenarios virtuales.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 1-12 ISSN 2550-6730

Referencias

[1] Organ. Mund. la Salud. "Salud mental". En: *2014* 1 ().

[2] Riva. "Departamento de Personalidad Artículo Monográfico La realidad virtual para el tratamiento de los trastornos emocionales: una revisión". En: *1998* ().

[3] Fiandra Fatharany y col. "Augmented reality application for cockroach phobia therapy using everyday objects as marker substitute". En: *2016 International Conference on Information & Communication Technology and Systems (ICTS)*. IEEE, 2016, págs. 49-52.

[4] Dana Horváthová, Vladimír Siládi y Eva Lacková. "Phobia treatment with the help of virtual reality". En: *2015 IEEE 13th International Scientific Conference on Informatics*. IEEE, 2015, págs. 114-119.

[5] Raquel Ellem Marcelino de Oliveira y Jauvane Cavalcante de Oliveira. "Virtual Reality System for the Treatment of Acrophobia". En: *2017 19th Symposium on Virtual and Augmented Reality (SVR)*. IEEE, 2017, págs. 74-77.

[6] Ana Paula Cláudio y col. "Virtual environment to treat social anxiety". En: *International Conference of Design, User Experience, and Usability*. Springer, 2013, págs. 442-451.

[7] João P. Costa, James Robb y Lennart E. Nacke. "Physiological acrophobia evaluation through in vivo exposure in a VR CAVE". En: *2014 IEEE Games Media Entertainment*. IEEE, 2014, págs. 1-4.

[8] Alex Armando Torres Bermúdez, Hugo Arboleda y Walter Lucumí Sánchez. "Modelo de Gestión y Gobierno de Tecnologías de Información en universidades de Colombia: Caso Instituciones de Educación Superior en el Departamento del Cauca". En: III (2014).

[9] Marc Davies y Victor Callaghan. "iWorlds: Building mixed reality intelligent environments using customisable 3D virtual worlds". En: *2010 Sixth International Conference on Intelligent Environments*. IEEE, 2010, págs. 311-314.

[10] BaÃ$\pm$os Rivera, Cristina Botella Arbona y Soledad Quero Castellano. "Tratamiento mediante realidad virtual para la fobia a volar: un estudio de caso". En: *Clinical and Health* 12.3 (2001), págs. 391-404.

[11] Rodrigo Braga y col. "Virtual reality as a support tool for the treatment of flying phobia: A pilot study". En: *2017 19th Symposium on Virtual and Augmented Reality (SVR)*. IEEE, 2017, págs. 65-73.

[12] E. Multissensorial y D. Presença. "Criação de Ambientes Virtuais de Simulação Imersivos para Terapia de Exposição Exposure Therapy". En: ().

[13] Teppei Tsujita y col. "Drop test for evaluating effect of cushioning material and servo gain on parachute landing impact using a small one-legged robot". En: *2017 IEEE International Conference on Robotics and Biomimetics (ROBIO)*. IEEE, 2017, págs. 2474-2479.

[14] Li Yaoyao y Jiang Chunlan. "Research on the Fall Points Spread of the Parachute-Bomb System". En: *2013 Fifth International Conference on Measuring Technology and Mechatronics Automation*. IEEE, 2013, págs. 937-940.

[15] Yanchao Fang y col. "The implementation of parachute jump commanding and simulation training system". En: *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*. Vol. 2. IEEE, 2010, págs. V2-518.

[16] Emmanuel Ferretty. "Redes en caída libre. Información, saber y confianza en la práctica de saltos tándem en paracaidismo". En: *11 Congreso Argentino de Educación Física y Ciencias 28 de septiembre al 2 de octubre de 2015 Ensenada, Argentina*. Universidad Nacional de La Plata. Facultad de Humanidades y Ciencias de la ..., 2015.

[17] Li Qizhong, Wang Ye y Wang Zhongqi. "Influencing Factors of Parachute-non-Bomb Trajectory in the Fuel-Air Explosives". En: *2017 Second International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*. IEEE, 2017, págs. 194-198.

[18] Dong Pyo Jang y col. "The development of virtual reality therapy (VRT) system for the treatment of acrophobia and therapeutic case". En: *IEEE Transactions on Information Technology in Biomedicine* 6.3 (2002), págs. 213-217.

[19] Grigore Burdea y col. "BrightArm™ therapy for patients with advanced dementia: a feasibility study". En: *2013 International Conference on Virtual Rehabilitation (ICVR)*. IEEE, 2013, págs. 208-209.

[20] Ceyda Duran Aygun y col. "Implementation Study of Parachute Training Simulator". En: *2019 6th International Conference on Electrical and Electronics Engineering (ICEEE)*. IEEE, 2019, págs. 307-311.

[21] Dimitrios Christopoulos y col. "Using Virtual Environments to Tell the Story:"The Battle of Thermopylae"". En: *2011 Third International Conference on Games and Virtual Worlds for Serious Applications*. IEEE, 2011, págs. 84-91.

[22] Qizhi Yin y col. "The software design of energy efficiency data acquisition and management of operational ships". En: *2017 4th International Conference on Transportation Information and Safety (ICTIS)*. IEEE, 2017, págs. 722-726.

[23] Juliana Martins Oliveira y col. "Complementary treatment for children with cerebral palsy based on virtual reality". En: *IEEE Latin America Transactions* 14.8 (2016), págs. 3820-3825.

[24] Dennis R. dela Cruz y Dion Michael M. Mendoza. "Design and development of virtual laboratory: A solution to the problem of laboratory setup and management of pneumatic courses in Bulacan State University College of Engineering". En: *2018 IEEE Games, Entertainment, Media Conference (GEM)*. IEEE, 2018, págs. 1-23.

[25] Sarthak Gadre y col. "Implementation and Design Issues for Augmented Reality Applications on Mobile Platforms". En: *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, 2018, págs. 1341-1344.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 12-27 ISSN 2550-6730

Recibido: 12/01/2020
Aceptado: 15/04/2020

Usabilidad de herramientas HCI que mejoran la capacitación en la gestión de emergencias.

Patricia Quiroz-Palma [1,2] M. Carmen Penadés [1] Ana-Gabriela Núñez [1,3]

[1]Universidad Politécnica de Valencia, Valencia-España,
[2]Universidad Laica Eloy Alfaro de Manabí, Manta-Ecuador,
[3]Universidad de Cuenca, Cuenca-Ecuador,
patquipa@dsic.upv.es, mpenades@dsic.upv.es, anunez@dsic.upv.es

RESUMEN
La efectiva interacción de los humanos con las máquinas es un aspecto importante en el desarrollo y mejoramiento de herramientas de software. Actualmente, el uso de los dispositivos electrónicos en las actividades diarias que realizan los seres humanos está en aumento. Estas herramientas no sólo deben ser seguras, útiles y efectivas, además se debe poner énfasis en la usabilidad y la experiencia del usuario. Este trabajo tiene como objetivo determinar los principios y técnicas usados en las herramientas actuales de capacitación. Para lograrlo, se realiza un análisis comparativo de las herramientas web existentes para la capacitación de usuarios. Además, desde el punto de vista de la interacción humano-computador (HCI), se estudian dos herramientas de capacitación CiET y Coursera, determinando los principios HCI que serán los indicadores de evaluación con el objetivo de mejorar las herramientas de software y en especialmente las destinadas para la capacitación en gestión de emergencias.
Palabras-clave: interacción humano-computador; HCI; gestión de emergencias; capacitación; entrenamiento; CiET.

ABSTRACT
The effective interaction of humans with machines is an important aspect in the development and improvement of software tools. Currently, the use of electronic devices in the daily activities performed by humans is increasing. These tools must not only be safe, useful and effective, but also emphasize usability and user experience. This work aims to determine the principles and techniques used in current training tools. To achieve this, a comparative analysis of existing web tools for user training is carried out. In addition, from the point of view of human-computer interaction (HCI), two training tools are studied, CiET and Coursera, determining the HCI principles that will be the evaluation indicators with the aim of improving the software tools and especially those designed for training in emergency management.
KEYWORDS: human-computer interaction; HCI; emergency management; training; CiET.

1. Introducción

En la vida cotidiana vemos muchos ejemplos de la interacción de los seres humanos con dispositivos electrónicos y sus herramientas de software, debdo a que muchas actividades o gestiones se han automatizado en dispositivos móviles o computadores. Es importante que estos sistemas cuenten con una interfaz amigable con el usuario, especialmente en las actividades y aspectos en los que el usuario tiene contacto. El diseño de la interfaz de usuario es muy importante en el desarrollo de sistemas informáticos y se requiere una perfecta armonía en la interacción humano-computador (HCI).
Las herramientas de Tecnologías de la Información (TI) deben ser lo más amigables para el usuario final; para ello se deben diseñar, evaluar e implementar adecuadamente. Para el usuario, la facilidad para interactuar con una herramienta de TI determina si le dará uso o simplemente escogerá otra herramienta con similares prestaciones.
Existen muchas herramientas para la gestión de emergencias, en las cuales debe prevalecer una interacción optima del usuario con las herramientas de TI dispuestas para las diferentes fases y actividades que comprende la gestión de emergencias. Es necesario que estas herramientas se desarrollen o mejoren teniendo en cuenta aspectos importantes como la seguridad, utilidad, efectividad, eficiencia y usabilidad[1].
Las herramientas para capacitación en gestión de emergencias son importantes para la adecuada preparación de los involucrados, debido a que de ello depende la efectividad de la ejecución de cada una de las fases (planificación, respuesta y análisis) de la gestión de emergencias. El apoyo de las herramientas de TI en la capacitación también es importante (y reduce los costos) para la mejora continua de la prevención de desastres, emergencias y reconstrucción [2].
El objetivo de este trabajo es identificar las mejores prácticas de diseño de interfaces y principios de HCI en las herramientas para la capacitación de gestión de emergencias y lograr con ello no sólo mejorar el entrenamiento y respuesta de los involucrados, sino optimizar las actividades realizadas en cada una de las fases de gestión de emergencias a través de herramientas que permitan la interacción de los humanos con los sistemas de una forma ágil y adecuada.
Este articulo está organizado como se indica a continuación. Sección 2, los trabajos relacionados con HCI, la capacitación en gestión de emergencias y las herramientas existentes. Sección 3, Diseño de interfaces y principios HCI. Sección 4, caso de estudio de dos herramientas que implementan los principios de HCI. Sección 5, discusión y finalmente, Sección 6, conclusiones y trabajos futuros.
A. HCI (Human-Computer Interaction)
Existen varias definiciones de HCI. [3] define que, la interacción humano-computadora (HCI) es la tecnología ciencia que investiga la comunicación entre los seres humanos y ordenador a través de la comprensión y el intercambio mutuos, lograr a las funciones de información de gestión, servicio y proceso para las personas.
[4] indica que HCI es un estudio de la interacción entre el sistema y los usuarios. La Interfaz hombre-computadora se refiere generalmente a la parte visible del usuario para comunicarse con el sistema y operar a través de las interfaces interactivas. Interacción humanizada entre el hombre y la computadora. HCI es una disciplina que comprende el diseño, evaluación e implementación de sistemas interactivos para el uso humano y con el estudio de fenómenos a través de ello[5]. Los aspectos importantes para considerar son:

- Seguridad
- Utilidad
- Efectividad
- Eficiencia
- Usabilidad

Para conseguir una buena usabilidad, los diseñadores deben lograr:

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 12-27 ISSN 2550-6730

1. Comprender cómo trabaja la gente y los factores que determinan el uso efectivo de ordenadores y dispositivos móviles.
2. Desarrollar las herramientas y técnicas que apoyen a los diseñadores y les asegure que los sistemas estarán disponibles para el usuario.
3. Conseguir que la interacción sea eficiente, segura y efectiva.

La interacción de entrada para los seres humanos son sus sentidos: vista, olfato, gusto, tacto y oído. Mientras que la interacción de salida son sus labios, dedos, ojos, cabeza y voz. [6], identifica 4 modos de interacción:

1. Interacción de datos: se refiere a los medios de transmisión de datos para comunicarse con las computadoras. Los modos de interacción de datos pueden realizarse por preguntas y respuestas, código de barras, reconocimiento óptico, entre otras formas.
2. Interacción de imágenes: se refiere al proceso que realiza la computadora para percibir e identificar las imágenes.
3. Interacción de voz: se refiere a la forma de reconocimiento y entendimiento de los computadores y humanos, es uno de los canales de información más importantes.
4. 4. Interacción inteligente: se refiere al reconocimiento inteligente para predecir las necesidades de los usuarios.

[7] determina que los factores relacionados con HCI y su implicación en los seres humanos son:

- Factores organizativos
- Factores de entorno
- Factores de salud
- Factores sobre el usuario
- Factores de confort
- Interfaz de usuario
- Tareas a realizar
- Restricciones
- Funcionalidad del Sistema
- Factores de la productividad

En el mundo real, estos factores se ven demostrados cuando vamos a un supermercado y el sistema con un lector de barras que no funciona, no existe un monitor para que el cliente vea el precio de cada artículo o no hay pago con tarjeta de crédito, hay que tener en cuenta que el usuario no es sólo el que usa el sistema sino también los clientes del supermercado [7].

B. Capacitación en Gestión de Emergencias

Los conocimientos impartidos en la capacitación ayudan a las personas no sólo a mejorar sus conocimientos, sino también a enfrentarse a las emergencias o a las situaciones que surgen de forma inesperada. Para evitar la obsolescencia de los conocimientos, la capacitación debe realizarse periódicamente según lo recomendado en el plan de capacitación. El plan de capacitación se basa en actividades que pueden ayudar a recopilar información sobre posibles nuevos sistemas y el apoyo de inversiones de recursos[8].

[9] indica que el contenido de la capacitación debe contener información teórica, experiencias y prácticas. [10]presenta los objetivos de aprendizaje, los cuales especifican los resultados del aprendizaje y la habilidad, y el conocimiento que se debe impartir al alumno. Además, [11] indica la necesidad de identificar el dominio de estudio a partir del cual se deben definir los contenidos del plan de formación. Desde nuestro punto de vista, una buena formación no sólo implica un conjunto de actividades a realizar periódicamente, sino que también incluye objetivos de aprendizaje, por lo que introducimos el concepto de plan de capacitación, que incluye ambos aspectos.

Las técnicas y herramientas que apoyan el proceso de capacitación pueden aplicarse para implementar un plan de capacitación. Por ejemplo, [12] indica que es necesario considerar los objetivos que se persiguen, el participante o grupo, su madurez, su entrenamiento, el entorno físico, el entorno psicológico y la capacidad del formador. Diferentes autores han propuesto diferentes técnicas de entrenamiento. Otro autor, [11], define técnicas como las entrevistas, la observación de los participantes, las historias de vida, las encuestas, los grupos de discusión, el diagnóstico participativo y la identificación de roles. [13] identifica otras técnicas como conferencias sobre teorías, demostración y capacitación, prácticas individuales y grupales. Las técnicas de capacitación son definidas por entrenadores expertos, quienes identifican seis técnicas, incluyendo entrenamiento en el trabajo, conferencias, juegos de roles, audiovisuales, aprendizaje programado y simulaciones.

La técnica de entrenamiento en el trabajo consiste en asignar nuevos empleados a los trabajadores experimentados o a los supervisores que se encargan del entrenamiento real. Existen varios tipos de esta capacitación, siendo los más conocidos: instrucción directa y rotación del puesto. La técnica de conferencia es práctica y fácil de implementar y es una forma rápida y fácil de proporcionar conocimientos a grupos grandes. Puede ir acompañada de materiales impresos para facilitar el aprendizaje. La técnica de juego de roles se utiliza para enseñar técnicas de venta, técnicas de entrevista, para dirigirse a grupos, resolver conflictos y lograr negociaciones o ocupar puestos de mayor responsabilidad y consiste en que los profesionales desempeñen roles de acuerdo con el puesto o las tareas que realizan. Las técnicas audiovisuales están relacionadas con la presentación de información a los empleados a través de técnicas audiovisuales como películas, circuito cerrado de televisión, cintas de audio o vídeo. La técnica de aprendizaje programado consiste en presentar un conjunto de preguntas o hechos para que el alumno los responda, luego revisa y compara las respuestas y repite las preguntas con respuestas erróneas hasta que todas hayan sido contestadas correctamente. Esta técnica es efectiva porque le da al empleado una retroalimentación inmediata sobre la exactitud de sus respuestas y sobre el aprendizaje que está logrando. La simulación es una técnica en la que los empleados aprenden en equipos reales o simulados la ejecución de sus tareas, por ejemplo, el manejo simulado de máquinas, vehículos o aviones. Este entrenamiento corrige errores sin poner a los estudiantes en situaciones peligrosas y es casi una necesidad en posiciones donde es demasiado caro o peligroso entrenar a los empleados directamente [14].

Dado que la tecnología influye en la eficacia de los contenidos y programas de formación, la organización debe planificar y organizar dichos contenidos de formación para que los participantes los motiven y los beneficien. Por ejemplo, la formación electrónica ofrece muchas oportunidades a las organizaciones empresariales y a los empleados en calidad de alumnos [15]. Entre las diversas oportunidades se encuentran el uso eficaz de la TI, la entrega de conocimientos y tecnologías actualizadas en cualquier momento, en cualquier lugar y a cualquier persona, el recorte de costos de la capacitación y la filosofía "justo a tiempo". Otras herramientas simulan juegos serios, como se explica en dos casos de estudio en [16]. El primer caso es una evacuación simulada de un barco en llamas y el segundo caso el simulador proporciona entrenamiento de respuesta en un accidente de tren.

En el ámbito de la gestión de emergencias, el objetivo de la formación es desarrollar las capacidades locales para responder a eventos inesperados y/o prevenir desastres. Por este motivo, es fundamental partir del conocimiento de las causas de los desastres y sus consecuencias, lo que nos lleva al análisis de riesgos. El análisis de las causas es necesario para determinar los diferentes factores que constituyen amenazas y vulnerabilidad para la población.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 12-27 ISSN 2550-6730

Figura 1: Dimensiones de la Capacitación para la Gestión de Emergencias (Adaptado de [17])

Ferradas identificó las dimensiones de la capacitación en áreas como Educación, Social, Técnica, Jurídica e Institucional, y Económica (Ver Figura 1). La educación se ocupa de la teoría de la gestión de riesgos y la planificación del desarrollo, los desastres y los medios de vida, la rehabilitación y la reconstrucción en la perspectiva del desarrollo y las normas mínimas para la ayuda humanitaria. La dimensión Social se refiere a la organización y el liderazgo, la ética y los valores, la memoria y la historia de los desastres, las percepciones del riesgo, las estrategias de prevención y adaptación, la cultura de prevención, las necesidades de información, los medios de comunicación, la comunicación informal, las redes de información y las campañas de información. La dimensión Técnica se relaciona con la evaluación de riesgos, la preparación de mapas de riesgos, el uso de bases de datos para la geo referenciación y los sistemas de información geográfica, los planes de preparación y respuesta a emergencias, las tecnologías para la prevención de desastres y la respuesta a emergencias, los sistemas de alerta temprana, la evaluación de daños y necesidades, la rehabilitación psicosocial, la gestión operativa de emergencias y la implementación de albergues temporales. La dimensión Jurídica e Institucional se refiere a la legislación vigente aplicable a la prevención y respuesta a los desastres, la legislación y reglamentación de la Defensa Civil, las leyes locales y las políticas estatales en materia de emergencias, las prioridades, los sistemas de apoyo y la distribución de la ayuda. Finalmente, la dimensión Económica se refiere al impacto económico de los desastres y la rentabilidad de las inversiones en desastres.

C. Herramientas de Capacitación y Entrenamiento para la Gestión de Emergencias Las herramientas interactivas que se han seleccionado y estudiado para este análisis comparativo incluyen a Udemy, Coursera, EvolMind y CiET (ver Tabla I).

Udemy es una plataforma de aprendizaje en línea. Está dirigido para adultos profesionales. A diferencia de los programas académicos MOOC conducidos por tradicionales cursos de trabajo creados por el colegio, Udemy utiliza contenido de creadores en línea para vender y así conseguir ganancias.

Coursera es una plataforma de educación virtual nacida en octubre de 2011 y desarrollada por académicos de la Universidad de Stanford con el fin de brindar oferta de educación masiva a la población.

EvolMind es un sistema de gestión del aprendizaje (LMS) que te facilita la creación, impartición, evaluación y análisis de formación online. Facilita la vida de tus alumnos y profesores con increíbles funcionalidades y potentes herramientas.

CiET es un framework que gestiona planes de capacitación basados en objetivos de aprendizaje, evalua-

ción de contenidos y retroalimentación del proceso formativo para lograr la mejora continua y el apoyo al proceso de enseñanza-aprendizaje a través de recursos internos y externos. Cada objetivo de aprendizaje debe incluir contenidos como texto, imágenes, videos, juegos, tutoriales, otros recursos (juegos serios) o recursos externos (fuente de datos) para permitir a los interesados adquirir los conocimientos necesarios para hacer frente a una emergencia. La capacitación puede realizarse de manera iterativa para lograr una mejora continua del aprendizaje. [18] aplicando los principios HCI, propone a través del Marco CiET (Mejora Continua de la Capacitación en Emergencias), su Modelo de Capacitación con la finalidad de lograr una formación personalizada de los involucrados y alcanzar un mayor de resiliencia para afrontar las emergencias y los desastres.

Tabla 1. EXTRACTO DE COMPARATIVA DE HERRAMIENTAS DE CAPACITACIÓN

CARACTERISTICAS	UDEMY	COURSERA	EVOLMIND	CIET
Capacitador	X			X
Aprendiz	X	X	X	X
Gestión de Emergencias				X
Genera Plan de Capacitación			X	X
Objetivos de Aprendizaje	X	X		X
Contenidos Personalizados				X
Técnicas de Capacitación	X	X	X	X
Herramientas IT Integradas				X
Evaluación de Aprendizaje	X	X	X	X
Retroalimentación				X
Resultados de Capacitación	X	X	X	X
Acceso Web	X	X	X	X
Gratis		X3		X
Link	www.udemy.com	www.coursera.org	www.evolmind.com	www.ciet.com

A pesar de que estas herramientas apoyan la capacitación en emergencias, no todas cumplen con los principios planteados para HCI. En la siguiente sección se realizará la comparación de dos herramientas que si cumplen con estos.

2. Diseño de interfaces y Principios HCI

Chao [6] define el diseño de las interfaces humano-computador en tres partes: diseño de estructura, diseño interactivo y diseño visual.

- Diseño de estructura o diseño conceptual: es el marco del diseño HCI, se construye a través de los requerimientos de usuarios y el análisis de tareas. Este diseño debe incluir los siguientes aspectos:
  a) Análisis de las necesidades de los usuarios
  b) Análisis del propósito de las tareas

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 12-27 ISSN 2550-6730

c) Diseño de tareas

- Diseño interactivo: se centra en hacer productos de software fáciles de usar y lograr que la comunicación y el diálogo de los humanos y el computador sea más armonioso. Esta etapa es el núcleo del diseño HCI. Comprende los siguientes aspectos:

  a) Determinar os tipos de diseño de la interacción
  b) Realizar el diseño de interacción y sus principios (orientado a personas, consistente, identificable y operacional, fácil de comunicar, rápido, retroalimentación y ayuda efectiva).

- Diseño visual: es el rendimiento de la interfaz, el diseño visual incluye aplicación de color, los procesos de gráficos e imágenes, tamaño y tipo de letras, deseño de páginas, etc. Para brindar al usuario interfaces amigables y fáciles de usar. Los principios del diseño visual son:

  a) Proporcionar una interfaz clara y coherente y que permita personalizar el contenido de la interfaz.
  b) Mejorar la función del ordenador de memorizar y reducir la carga de la memoria a corto plazo del usuario.
  c) Proporcionar más funciones como predeterminadas, deshacer y rehacer.
  d) Proporcionar más atajos de la interfaz.
  e) Respetar la experiencia pasada de los usuarios.
  f) Mejorar la estimulación visual de los símbolos gráficos a través de la aplicación de colores.

[3] determina los siguientes principios para el diseño de HCI de herramientas de capacitación web

a) Funcional, Directa y Fácil de usar.
b) La interacción debería traernos felicidad emocional
c) Seguro y Estable
d) Razonable, Eficiente y Consistente.

Las estrategias especiales de diseño de HCI para la capacitación a través de sitios web, se deben considerar tres aspectos siguientes: modales de interacción, principios de diseño de interacción y proceso de diseño de interacción. En base a lo anterior podemos asegurar que el diseño adecuado de las interfaces aplicando los principios de HCI es uno de los aspectos más importantes en el desarrollo de herramientas de software, debido a que proporciona fiabilidad y facilidad de uso que determinan la aceptación de la herramienta por parte de los usuarios.

3. Caso de Estudio: CiET vs Coursera

El análisis de la aplicación de HCI para la capacitación en emergencias se ha llevado a cabo con dos herramientas sin costo: Coursera y CiET, las cuales se describen a continuación.

A. CiET
Aunque algunas herramientas apoyan la capacitación en emergencias, el Marco CiET (Mejora Continua de la Formación en Gestión de Emergencias), difiere de las demás porque permite la evaluación y la

capacitación continua y personalizada para mejorar la capacitación. [18] a definido el modelo de capacitación para la gestión de emergencias, denominado modelo CiET. Este modelo permite personalizar los contenidos formativos de cada actividad y fase de emergencia para cada uno de los participantes. La importancia de una formación óptima se traduce en una mayor capacidad de recuperación en la gestión de emergencias, así como en la reducción del número de víctimas y de los costes derivados de un suceso inesperado.
El primer paso en la construcción de un plan de capacitación es identificar los parámetros generales, tales como las dimensiones y técnicas de la capacitación, las fases y actividades de la gestión de emergencias y los objetivos de aprendizaje esperados.
El segundo paso considera la importancia de la preparación de los participantes en la gestión de emergencias. Nos basamos en las dimensiones del entrenamiento de Ferradas y en las técnicas y expertos entrenadores de Fernández para definir un modelo de capacitación que enfatiza la personalización de los contenidos del entrenamiento para cada una de las actividades de cada fase, considerando tres fases: pre-desastre, respuesta y post-desastre. Identificamos los principales contenidos que se impartirán en el proceso de formación sobre las actividades de las fases de gestión de emergencias, como se muestra en la Figura 1. En la fase de planificación o pre-desastre, los participantes deben ser entrenados para identificar el tipo de emergencias, identificar los medios de protección, conocer las estructuras de los edificios, conocer el plan de emergencia, conocer las regulaciones legales e institucionales de la organización, detectar crisis, realizar análisis de riesgo e identificar una alerta (alerta de crisis). En la fase de respuesta, los participantes deben ser entrenados en temas vitales como el conocimiento de las rutas de evacuación, la identificación de señales y el uso de extintores. El equipo de respuesta también debe estar capacitado para utilizar los equipos de comunicación y rescate y para prestar primeros auxilios y actuar de manera eficiente hasta el retorno a la normalidad. En la fase de análisis o posterior al desastre, los participantes deben ser capacitados para brindar apoyo psicológico a las víctimas, analizar los costos de los daños, mejorar su resiliencia a los desastres e identificar los riesgos futuros.
El tercer paso fue identificar a los participantes en el proceso de capacitación, para lo cual nos referimos a la siguiente clasificación de involucrados: organización, planificadores, trabajadores, equipo de respuesta y ciudadanos definidos en el Marco Que [15]. En el proceso de capacitación se identifican dos roles, el del capacitador y el del aprendiz. La organización, los planificadores y los intervinientes pueden desempeñar el papel de capacitador y todas las partes interesadas cumplen el papel de alumno. También puede haber un capacitador externo, que es un experto en el tema a capacitar y que no forma parte de las partes involucradas. En la Tabla 1 se definen las responsabilidades de cada una de las partes interesadas y su papel en el proceso de capacitación. El capacitador es un participante activo en este proceso; este papel puede ser desempeñado por algunas de las partes interesadas (organización, planificadores, equipos de respuesta). También puede requerirse un experto externo, que debe ser un profesional del tema. Todos los participantes son partes interesadas que han sido capacitados en el proceso de capacitación.

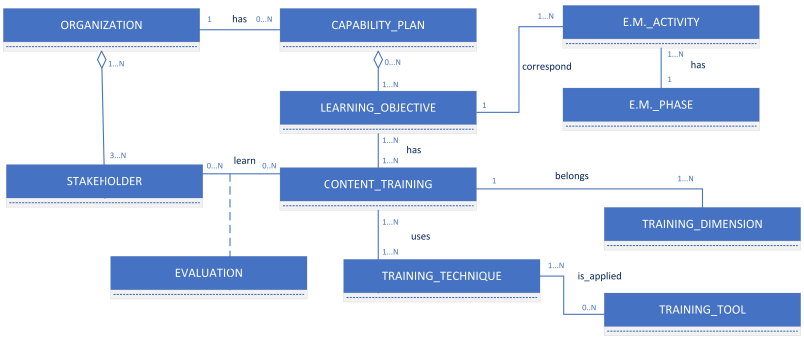

Figura 2: Modelo de Capacitación de CiET (Extraído de Quiroz-Palma et al., 2019a)

El cuarto paso fue relacionar a las partes interesadas que participan en la formación con el contenido y la

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 12-27 ISSN 2550-6730

dimensión de la misma. Es importante tener claros los contenidos, la dimensión a la que pertenecen y las personas que deben ser capacitadas, ya que una formación adecuada puede reducir los costos y mejorar la resiliencia (Anónimo, 2017) de las personas en situaciones de emergencia.
La Figura 2 resume el modelo conceptual de CiET propuesto como un diagrama de clase UML. Un plan de capacitación (representado por la clase CAPABITY_PLAN) es un conjunto de objetivos de aprendizaje (clase LEARNING_OBJECTIVE) relacionados con las fases de la gestión de emergencias (clase EM_PHASE) con sus respectivas actividades (clase EM_ACTIVITY). Los contenidos formativos (clase_TRAINING_CONTENT) se especifican en cada una de las actividades de gestión de emergencias, según la dimensión (clase_DIMENSIÓN_TRAINING) a la que pertenecen. Para cada contenido se pueden aplicar una o varias técnicas (clase TRAINING_TECHNIQUE) y herramientas informáticas (clase TRAINING_TOOL). Apoyar el aprendizaje de los involucrados (clase STAKEHOLDER) de la organización (clase ORGANIZATION) a través de la evaluación (clase EVALUATION) proporciona retroalimentación y la formación continua de los involucrados.

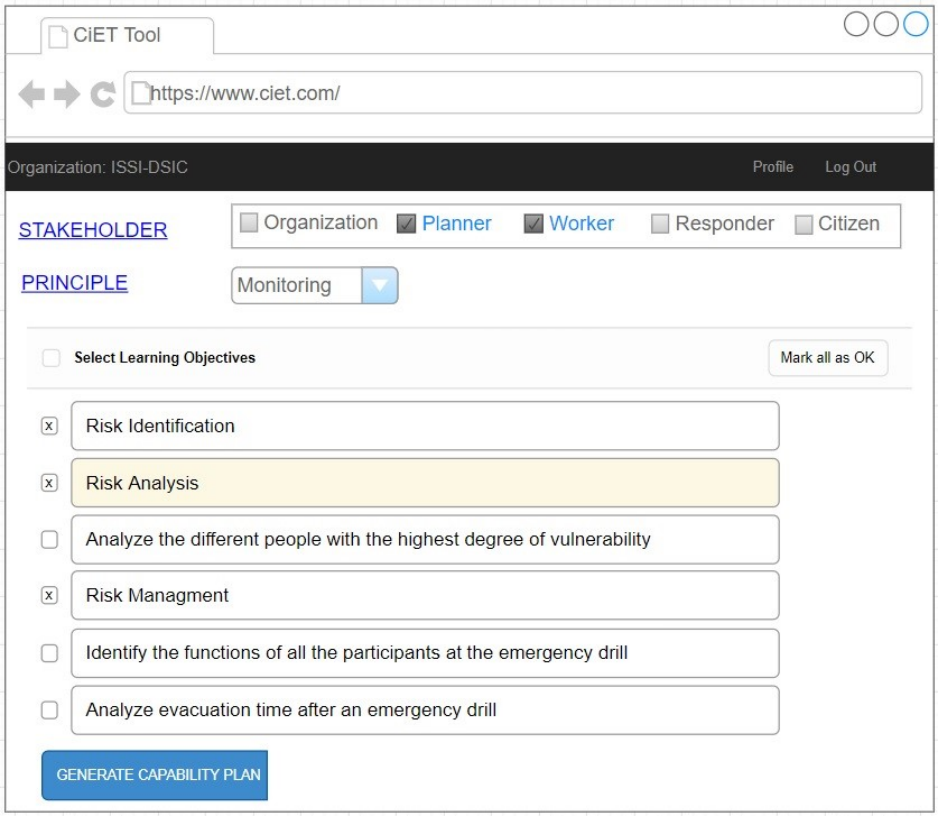

Figura 3: Interfaz CiET

Una organización define los planes de capacitación personalizados de los grupos de interés de acuerdo con los objetivos de aprendizaje establecidos en las actividades de gestión de emergencias seleccionadas (Ver Figura 3). El aspecto más relevante del plan de capacitación es evaluar los contenidos de la formación y medir el cumplimiento de los objetivos de aprendizaje establecidos. Si los contenidos de la capacitación y los objetivos de aprendizaje no se cumplen, se debe reforzar el contenido de la capacitación y repetir la evaluación para proporcionar retroalimentación al proceso de aprendizaje y rediseñar el plan de capacitación si hay deficiencias en los contenidos u objetivos de aprendizaje irreales.
La persona encargada de generar los planes de capacitación selecciona a los actores a capacitar y filtra

el principio QuEP a utilizar. Para generar el plan de capacitación, se seleccionan los objetivos de aprendizaje recomendados por el QuEP, así como el respectivo porcentaje de cumplimiento obtenido. Un plan de capacitación puede consistir en uno o más objetivos de aprendizaje como se muestra en la Figura 3.

B. Coursera

Coursera es una plataforma e-learning fundada por los profesores en ciencias de la computación de la Universidad de Standford, Andrew Ng y Daphne Koller en octubre de 2011 con el lanzamiento de dos cursos gratuitos,"Aprendizaje automático" ,"Introducción a las bases de datos". Una de sus aplicaciones más sobresalientes fue el lanzamiento de Coursera para refugiados mediante el convenio de Coursera y el Departamento de Estado de los Estados Unidos de Norteamérica. Este último apoyará el proyecto al ofrecer los cursos certificados de forma gratuita en los consulados y embajadas.

Entre las facilidades ofrece el aprendizaje de habilidades, prepararse para una carrera, obtener un certificado y mejorar una organización mediante la capacitación. Coursera permite la capacitación en diferentes campos:

- Artes y Humanidades,
- Negocios
- Ciencias de la Computación
- Ciencias de Datos
- Tecnologías de la Información
- Salud
- Matemáticas y Lógica
- Ciencias Físicas e Ingeniería
- Ciencias Sociales

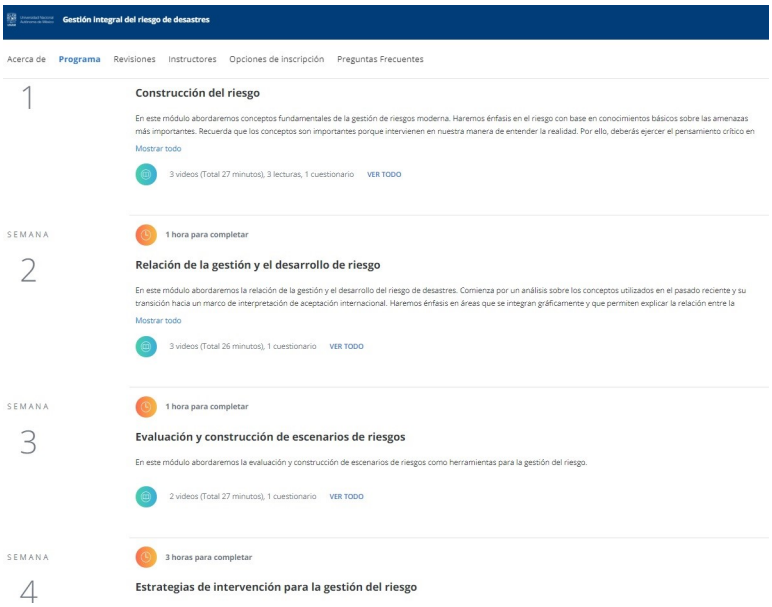

Figura 4: Interfaz Coursera

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 12-27 ISSN 2550-6730

Los cursos son ofertados por Universidades colaboradoras en el proyecto de capacitación. Es decir, los cursos y sus contenidos ya vienen definidos por la institución ofertante del mismo, como se observa en la Figura 4.

C. Análisis comparativo: CiET Vs Coursera

Estas dos plataformas de capacitación tienen características generales muy comunes entre sí, como lo vimos en la Tabla I. Para evaluar las características se definió un caso de estudio para ambas plataformas, el mismo que consistía en un curso de Gestión de Riesgos para Emergencias. En CiET, el capacitador experto generó el plan de capacitación con los contenidos referentes a la Gestión de Riesgos para Emergencias (Ver Figura 3). Mientras, en Coursera encontramos un curso ofrecido por la Universidad Autónoma de México, que responde al nombre Gestión Integral del Riesgo de Desastres (Ver Figura 4). Ambas herramientas son fáciles de usar, seguras y eficientes. A diferencia de Coursera, CiET es más razonable, directa y consistente en la gestión de emergencia y los roles de los involucrado. Mientras que en Coursera se puede generar un certificado al final del curso, avalado por la Universidad oferente.

Se evaluaron las interfaces de contenidos de ambas plataformas, tomando como indicadores a los principios de HCI enfatizados en el diseño de Interfaces de usuario para la interacción humano-computador. En la Figura 5 podemos observar unos de los contenidos de CiET y en la figura 6 uno de los contenidos de Coursera.

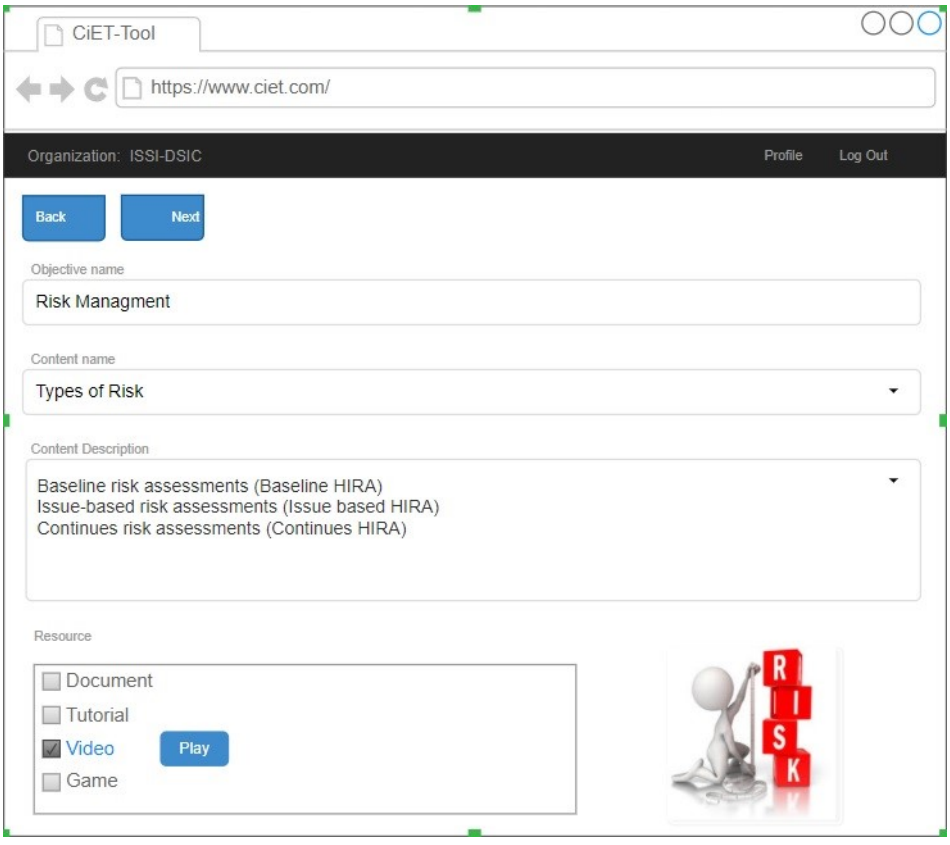

Figura 5: Contenido de CiET

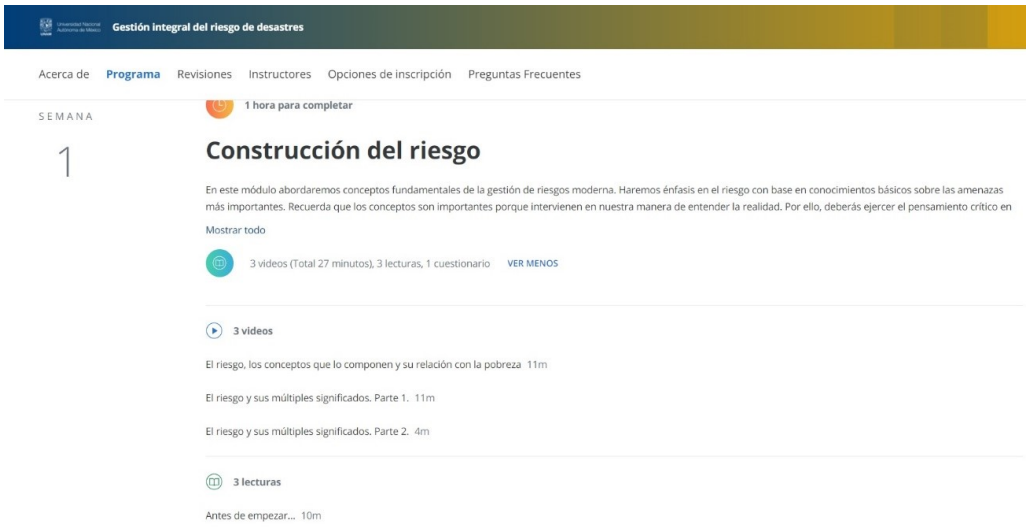

Figura 6: Contenido de Coursera

En la tabla II se resume la evaluación de CiET y Coursera con respecto a los principios de HCI planteados por [3], a los que le hemos agregado dos principios más con respecto al campo de estudio que en nuestro caso es la gestión de emergencias.

Tabla 2. COMPARATIVA DE PRINCIPIOS HCI EN HERRAMIENTAS DE CAPACITACIÓN

Principios HCI	COURSERA	CIET
Funcional	X	X
Directa		X
Fácil de usar	X	X
La interacción trae felicidad emocional		
Seguro	X	X
Estable	X	X
Razonable		X
Eficiente	X	X
Consistente		X
Especializado en gestión de emergencias		X
Maneja roles de involucrados en gestión de emergencias		X

4. Discusión

En la sección anterior se presentaron dos herramientas, las cuales son funcionales, seguras, estables y fáciles de usar. Sin embargo, CiET es más directa y especializada en la gestión de emergencias, empleando los roles de los involucrados planteados en el Marco QuEP para la mejora de la calidad en la gestión de planes de emergencias en una organización. Por otra parte, Coursera genera certificados con costo, porque no es una capacitación directa, sino que es intermediario entre el usuario y las Universidades que ofertan los cursos. Entre otras ventajas que CiET tiene sobre otras herramientas, es que cumple con los principios HCI que coinciden varios autores. Además, podemos enfatizar que CiET se puede integrar a

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 12-27 ISSN 2550-6730

QuEP u otros marcos de evaluación de las organizaciones y tomar sus datos de relación para generar los planes de capacitación.

5. Conclusiones y Trabajos Futuros

De acuerdo con los aspectos analizados en el diseño de HCI de las herramientas de capacitación analizadas Podemos concluir que la herramienta CiET cumple con los lineamientos de diseño para interfaces HCI para una mejor interacción de los usuarios con las máquinas, siendo una herramienta directa con funcionalidad, estabilidad, seguridad y facilidad de uso. Además de ser amigable con el usuario logrando la aceptación de todos los involucrados en la gestión de emergencias.
Otro aspecto importante que se debe destacar en la evaluación de estas herramientas es la especialización de la herramienta CiET para la capacitación en gestión de emergencias, donde se establece la capacitación personalizada para cada uno de los roles de los involucrados en la gestión de emergencias definidos en el marco QuEP (Anónimo, 2015), por ello la herramienta es especializada en este campo.

Como trabajos futuros, se plantea mejorar el diseño de las interfaces de CiET para lograr la felicidad emocional que es uno de los principios que no cumplían ambas herramientas, además de generar certificado avalado por la organización que aplica la capacitación con el marco CiET.

Agradecimientos
El trabajo de P. Quiroz-Palma es parcialmente soportado por la Universidad Laica Eloy Alfaro de Manabí, el trabajo de M. C. Penadés es parcialmente financiado por MINECO bajo el proyecto CALPE (TIN2015-68608-R), y el trabajo de A.G. Núñez es parcialmente soportado por el Departamento de Recursos Hídricos y Ciencias Ambientales, Universidad de Cuenca.

Referencias

[1] Klaus Kremer. "Critical human factors in UI design: How calm technology can inform anticipatory interfaces for limited situational awareness." En: ().

[2] Raj Prasanna, Lili Yang y Malcolm King. "Evaluation of a software prototype for supporting fire emergency response". En: *Proceedings of the 8th International ISCRAM Conference–Lisbon, Portugal*. 2011.

[3] Peng Bian, Yi Jin y Nairen Zhang. "Research on human-computer interaction design for distance education websites". En: *2010 5th International Conference on Computer Science & Education*. IEEE, 2010, págs. 716-719.

[4] Lu Song y Fuan Wen. "The Human-Computer Interaction Design and Research of Virtual Experiment". En: *2014 Sixth International Conference on Intelligent Human-Machine Systems and Cybernetics*. Vol. 1. IEEE, 2014, págs. 50-53.

[5] Jakob Nielsen. "Computer-support cooperative work". En: *ACM SIGCHI Bulletin* 19.1 (1987), págs. 54-61.

[6] Gong Chao. "Human-computer interaction: process and principles of human-computer interface design". En: *2009 International Conference on Computer and Automation Engineering*. IEEE, 2009, págs. 230-233.

[7] Jenny Preece y col. *Human-computer interaction*. Addison-Wesley Longman Ltd., 1994.

[8] Cheryl M. Strube y Jeff R. Loren. "Portfolio influences on air force capabilities-based assessment and capabilities-based planning activities". En: *2011 6th International Conference on System of Systems Engineering*. IEEE, 2011, págs. 83-88.

[9] Ying Xing y Shengde Hu. "Following Construction Study of One Village One College Student Training Plan in Heilongjiang Province". En: *2010 International Conference on e-Education, e-Business, e-Management and e-Learning*. IEEE, 2010, págs. 436-439.

[10] Syaamantak Das. "Cognitive Level Analysis in a Learning Cycle". En: *2018 IEEE 18th International Conference on Advanced Learning Technologies (ICALT)*. IEEE, 2018, págs. 449-451.

[11] Pedro Ferradas, Adolfo Vargas y Giovanna Santillán. *Metodologías y herramientas para la capacitación en gestión de riesgo de desastres*. Soluciones prácticas, 2007.

[12] J Fernández. "Dinámicas de grupos y técnicas participativas". En: *Lima* (2005).

[13] Pan Suixiong. "Practice and Quest of the Teacher's Training in Educational Technique Ability". En: *2009 First International Workshop on Education Technology and Computer Science*. Vol. 2. IEEE, 2009, págs. 780-784.

[14] M. M. Adibi. "Bulk Power System Restoration Training Techniques". En: (2000).

[15] Hardeep Singh y Bikram Pal Singh. "E-Training: An assessment tool to measure business effectiveness in a business organization". En: *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2015, págs. 1229-1231.

[16] Ilona Heldal. "Simulation and serious games in emergency management: experiences from two case studies". En: *2016 22nd International Conference on Virtual System & Multimedia (VSMM)*. IEEE, 2016, págs. 1-9.

[17] Patricia Quiroz-Palma, Ma Carmen Penadés y Ana-Gabriela Núñez. "TiER: A Serious Game for Training in Emergency Scenarios". En: *2019* ().

[18] Patricia Quiroz-Palma, Ma Carmen Penadés y Ana-Gabriela Núñez. "Towards a Capability Model for Emergency Training Improvement". En: *2019* ().

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 27-33 ISSN 2550-6730

Recibido: 13/02/2020
Aceptado: 15/04/2020

APLICACIÓN DE LAS TIC EN LA ENSEÑANZA DEL ELECTROMAGNETISMO PARA CARRERAS DE INGENIERÍA.

Ramiro Serrano Guerrero [1]

[1]Universidad de Holguín,

RESUMEN
El trabajo tiene como objetivo mostrar la concepción de un material didáctico multimedia para el proceso de enseñanza-aprendizaje de temas de Electromagnetismo de la asignatura Física II en las carreras de Ingeniería Mecánica, Ingeniería Civil e Ingeniería Industrial. Contiene el desarrollo de las temáticas con ilustraciones, modelos animados, cuadros resúmenes, ejercicios y aplicaciones que motivan a los estudiantes y permiten el estudio independiente y el uso por parte de los profesores para el desarrollo de actividades docentes. Los materiales están concebidos sobre la base de un soporte didáctico. Además del aporte práctico, en el orden teórico presenta una relación estrecha con el uso de modelos y simulaciones para la comprensión de las leyes, fenómenos y procesos. Se ha comprobado que estos medios incrementan la efectividad del aprendizaje y disminuyen el tiempo presencial del profesor, tomando en cuenta también otras temáticas que los autores han desarrollado en igual soporte desde unos 12 años atrás. Los resultados del proceso de enseñanza aprendizaje con el auxilio de estos medios fueron superiores a los esperados en cuanto a calidad, cumplimiento de los objetivos, resultados evaluativos y nivel de satisfacción de los estudiantes. La multimedia ha sido construida usando fundamentalmente Microsoft Power Point y sin grandes pretensiones profesionales, resulta útil para estudiantes y profesores, estimula el uso de las TIC y muestra que es posible incrementar el uso de las computadoras como medio de enseñanza sin grandes conocimientos informáticos.
Palabras-clave: Electromagnetismo; enseñanza-aprendizaje, multimedia.

ABSTRACT
The objective of the work is to show the conception of a multimedia didactic material for the teaching-learning process of Electromagnetism subjects of the Physics II subject in the careers of Mechanical Engineering, Civil Engineering and Industrial Engineering. It contains the development of the themes with illustrations, animated models, summary tables, exercises and applications that motivate students and allow independent study and use by teachers for the development of teaching activities. The materials are conceived on the basis of a didactic support. In addition to the practical contribution, in the theoretical order it presents a close relationship with the use of models and simulations for the understanding of laws, phenomena and processes. It has been proven that these means increase the effectiveness of learning and decrease the teacher's classroom time, also taking into account other topics that the authors have developed in the same format since about 12 years ago. The results of the teaching-learning process with the help of these means were higher than expected in terms of quality, achievement of objectives, evaluation results and level of student satisfaction. The multimedia has been built using mainly Microsoft Power Point and without great professional pretensions, it is useful for students and teachers, it stimulates the use of ICT and shows that it is possible to increase the use of computers as a means of teaching without great computer knowledge.
KEYWORDS: Electromagnetism; teaching-learning, multimedia.

1. Introducción

El desarrollo y evolución de las tecnologías informáticas, como objeto de estudio es muy importante para la enseñanza, también como herramienta de trabajo, pero más aún como un medio que ayuda notablemente a incrementar las potencialidades educativas. Con estos equipos informáticos interactivos, un estudiante podrá consultar el texto, ver además fotografías, animaciones o un vídeo sobre el tema e interactuar durante la adquisición de conocimientos y la realización de ejercitación. Con los avances tecnológicos, el proceso de enseñanza-aprendizaje tiende a ser una tarea más grata y accesible.[1]
En este trabajo se presentan seis temas en forma de materiales multimedia del contenido del curso de electromagnetismo. Los materiales incluyen ilustraciones, animaciones, cuadros resúmenes, se usan en su elaboración modelos y simulaciones, posibilitan interacción entre estudiante y computadora. Constituyen una vía para contribuir con el uso de las TIC en la enseñanza de la física en carreras de Ingeniería, tanto en el estudio independiente, así como para herramienta del profesor en actividades presenciales.
En el desarrollo de este trabajo, en primer lugar se realiza la búsqueda de los fundamentos teóricos necesarios para concebir una multimedia didáctica y para su posterior elaboración. La exploración en cuanto al estado y uso de estos medios informáticos en Física para Ingeniería, permitió justificar la ejecución del trabajo. La multimedia fue aplicada en las carreras de ingeniería mecánica, ingeniería civil e ingeniería industrial de la universidad de Holguín y valorados sus resultados.
Este medio pretende reunir características tales que motiven a los estudiantes y permitan el estudio de las temáticas en diferentes momentos del desarrollo del proceso de enseñanza-aprendizaje, pues puede utilizarse en el inicio, durante el desarrollo y como consolidación de las temáticas respectivas.

2. Desarrollo

El uso de las TIC ocupa actualmente un importante lugar en el proceso de enseñanza-aprendizaje. En particular, el uso de la computadora, el gran volumen de información que genera el creciente uso de Internet y el trabajo con páginas Web se integran actualmente con mayor frecuencia en diferentes estrategias de aprendizaje [2].
La actividad docente y en particular la clase, en la actualidad se modernizan de modo creciente con la utilización de los más variados métodos y medios en el proceso de enseñanza-aprendizaje, con los procedimientos que pueden utilizar los estudiantes para aprender y con el uso de la computación. Lo anterior determina modificaciones en las formas de presentar los contenidos, en las habilidades que se deben desarrollar y por tanto en la formación integral de los estudiantes. La introducción de las nuevas tecnologías ayuda en la resolución de la contradicción entre el volumen creciente de información que se debe transmitir y el tiempo escolar disponible[3].
El uso de la computadora permite la interactividad con el usuario durante el estudio independiente teniendo en cuenta que puede recibir información, procesarla y dar una respuesta, además posibilita que el propio estudiante personalice el aprendizaje.
Según la literatura consultada y la experiencia de los autores, esta herramienta brinda gran cantidad de posibilidades y bondades en un gran espectro de la actividad docente, mientras que en el caso particular que aborda este trabajo pueden plantearse las siguientes:

- Muchos fenómenos naturales no pueden ser visualizados, como los de orden molecular, atómico o a niveles más reducidos del micro mundo. Sin embargo con la computadora y con el uso del software adecuado se posibilita realizar modelos animados que facilitan notablemente la actividad del docente y la comprensión de los fenómenos.
- Aún cuando se trata de fenómenos o procesos macroscópicos, existen situaciones que no pueden ser llevadas la sala docente, por eso en estos casos también la simulación informática puede jugar un papel importante.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 27-33 ISSN 2550-6730

- En casos de ausencia de recursos de laboratorio para demostraciones experimentales, pueden usarse presentaciones virtuales, aunque es importante aclarar que nunca la virtualización puede sustituir completamente una demostración real.
- Además una demostración real o una práctica de laboratorio pueden ser analizadas, explicadas, modeladas y complementadas con una presentación virtual, incluyendo fundamentos teóricos de fenómenos macroscópicos y microscópicos.

Los modelos que representan objetos o fenómenos constituyen un método del conocimiento. Los conocimientos se transmiten con el uso de modelos. La posibilidad de presentar modelos gráficos estáticos o animados, constituye una notable ayuda en el desarrollo de una actividad docente presencial y esto se facilitada notablemente usando la computadora como medio de enseñanza.[4]

Concepción didáctica de la multimedia

En la aplicación de las TIC en el campo educativo es necesario tener en cuenta que el asunto es más didáctico que tecnológico. El potencial educativo de un medio no depende tanto de sus características y potencialidades intrínsecas, sino de la forma como son utilizados para conseguir los fines educativos[5]. Es por eso que los materiales multimedia elaborados fueron concebidos de acuerdo con la didáctica a partir de la consulta de diversos materiales, sobre los que se hace un breve resumen a continuación.

Una multimedia debe reunir un conjunto de características para que proporcione ambientes instructivos efectivos para el aprendizaje [6], como son: proporcionar a los estudiantes la posibilidad de participar activamente en el proceso de aprendizaje e incentivar esta participación; permitir que el estudiante dirija por sí mismo su aprendizaje, se involucre en la planificación de sus actividades; facilitar la interactividad y el "aprender haciendo" por encima de otros procedimientos en los que la implicación del aprendiz es menor; considerar problemas y situaciones reales como puntos de partida, haciendo sentir al estudiante que la actividad que realiza está estrechamente ligada a sus necesidades; permitir centrar al estudiante en la realización de tareas, la solución de problemas y la consecución de metas; contener recursos para llamar la atención del estudiante y facilitar la percepción de los factores esenciales del contenido (tipos de letras, diagramas, animaciones, colores, etc.); ser capaz de despertar el interés del estudiante; ofrecer herramientas de aprendizaje para la tarea inmediata y de funcionamiento intuitivo; situar el aprendizaje en el contexto, actividad y cultura habituales del estudiante.

Los anteriores constituyen requisitos generales de los cuales se derivan situaciones específicas, como son los siguientes criterios generados en el desarrollo de este trabajo:

- La información contenida en cada pantalla o diapositiva de la multimedia no debe ser cargada en la medida que produzca cansancio y disminuya el interés.
- Cada diapositiva deberá tener una información terminada o parcialmente terminada de modo que estimule la busca de nuevos elementos que a su vez sean accesibles mediante hipervínculos.
- Las animaciones y otros elementos anexos que aparecen en las diapositivas no deben constituir adornos que desvíen la atención. Sus funciones deben ser modelar los fenómenos objeto de estudio.
- Aprovechar la oportunidad que ofrece esta tecnología para visualizar modelos que representan fenómenos o procesos y que pueden ser animados representando lo que no se puede ver a simple vista.

Las funciones didácticas en la concepción de un medio de enseñanza, constituye otro elemento esencial. A partir de la literatura consultada , se profundizó en cuanto a las funciones didácticas y se procuró sustentar el trabajo en las mismas: La función instructiva tiene que ver con las posibilidades que ofrece el proceso para que los estudiantes se apropien de conocimientos, habilidades y capacidades intelectuales necesarias para un desempeño profesional determinado, pero más aún para aprender a aprender. La función educativa tiene que ver con el desarrollo de valores, actitudes y la personalidad de los estudiantes. La función desenvolvedora tiene que ver con el desarrollo de capacidades creativas del sujeto, con el desarrollo de capacidades para aprender a transformar.

3. Introducción en la práctica docente y desarrollo del trabajo

Durante el curso 2005-06 se inicia el trabajo de elaboración de estos materiales multimedia, primeramente para Física III, luego para Física II. Inicialmente, a partir de una situación provocada por un fenómeno natural (paso de un huracán), se impuso buscar procedimientos y medios que posibilitaran desarrollar un curso en un tiempo limitado usando un método de enseñanza semipresencial. La aplicación de estos medios resultó muy efectiva, teniendo en cuenta que facilitaron desarrollar todo el contenido del programa de física III para Ingeniería Mecánica con buenos resultados docentes y satisfacción de los estudiantes. Las presentaciones animadas contribuyeron notablemente durante el proceso de municipalización de las carreras universitarias para estudiantes y profesores de esas sedes municipales.
Estos materiales multimedia fueron incorporados al registro de derecho de autor y a partir de ese momento se usan sistemáticamente por los profesores en el desarrollo de actividades docentes presenciales y por los estudiantes para el estudio independiente, incluyendo otras especialidades además de Ingeniería Mecánica, habiendo trascendido además a otros centro de educación superior. Los trabajos están en la plataforma informática de la UHo “Oscar Lucero Moya” y del MES.
En los años posteriores se ha trabajado en la elaboración de este tipo de medios para Física II (Electromagnetismo). El trabajo que ahora se presenta, está constituido por seis temas en multimedia del curso de Física II:

- Las cargas eléctricas y el campo electrostático.
- Conducción de la corriente eléctrica en metales.
- El campo magnético. Ley de Ampere.
- El fenómeno de inducción electromagnética. Ley de Faraday.
- Oscilaciones electromagnéticas.
- Ecuaciones de Maxwell y ondas electromagnéticas.

Muchos fenómenos de los que derivan los conceptos y leyes de este contenido son fundamentalmente interacciones en el mundo microscópico, por lo que el uso de modelos animados, todos elaborados en el desarrollo de este trabajo, resulta extremadamente útil para trasmitir los conocimientos, para la comprensión del asunto, así como para el desarrollo de habilidades y capacidades de razonamiento. Por otra parte, estas temáticas presentan importantes nexos con conocimientos propios de la profesión del ingeniero y con asignaturas de la especialidad.
En el año 2013 en la Universidad de Holguín (UHo), después de explorar por observación directa y realizar entrevistas a los profesores en cuanto a la existencia de recursos de este tipo y la necesidad de los mismos para apoyar el proceso docente, se detecta que como material en soporte informático se contaba con libros digitalizados, indicaciones y orientaciones para los estudiantes para clases prácticas y laboratorios y prácticas de laboratorio virtuales fundamentalmente, sin embargo no con materiales en forma de multimedia para apoyar las actividades docentes presenciales y estimular el estudio independiente con elementos animados y amenos. A partir de estas circunstancias se inicia la investigación para este trabajo y son llevados los temas llevados a multimedia mediante un trabajo intensivo y sistemático.

4. El Material Didáctico Multimedia

El software utilizado es fundamentalmente Microsoft Power Point de Microsoft Office. Este software permite elaborar multimedia sin la necesidad de profundos conocimientos informáticos mediante la interface de usuario, aunque sí con un poco de creatividad e imaginación. Lo qué más se necesita es el conocimiento del contenido que se va a tratar, su tratamiento a la luz de la didáctica y su fundamento

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 27-33 ISSN 2550-6730

psicopedagógico, que son los elementos fundamentales para lograr una herramienta que cumpla con los requisitos necesarios para poder considerarla un medio de enseñanza.
Microsoft Power Point permite representar una gran diversidad de figuras, en una y dos dimensiones, simular tres dimensiones, usar los colores deseados, animar las figuras, simular infinidad de procesos, construir modelos animados, etc. Tiene posibilidades de establecer hipervínculos, insertar imágenes, películas y sonidos, vídeos, gráficos, elaborar interactividades.
Es importante tener en cuenta que no deben usarse animaciones y otras posibilidades para adornar. Usar esencialmente las animaciones personalizadas y no las pre-diseñadas, fue una forma muy usada y todo indica que ayuda mucho más en la creatividad del elaborador.
Lo materiales multimedia aparecen en soporte informático que se anexa a este trabajo y constituye la esencia de la investigación, pues se trata del producto más importante que deriva de ella.
Características generales de la multimedia:

- En cada diapositiva se brinda una información concreta y terminada, pero se presentan mediante hipervínculos diversas opciones de navegación: regresar la página principal, lograr más información del asunto objeto de estudio, etc.,
- En la mayoría de los casos, los contenidos se presentan mediante modelos animados que simulan fenómenos microscópicos, variaciones de los parámetros, acciones externas sobre los sistemas, etc. En la elaboración de las diapositivas se tuvo en cuenta un empleo adecuado de modelos, simulaciones y animaciones para mejor comprensión, para el desarrollo de procesos mentales, así como para el desarrollo de la imaginación.
- La información que contiene cada diapositiva se limita a un volumen que no resulte muy extenso, de modo que otros aspectos del contenido se proponen al estudiante mediante hipervínculos. Esto permite centrar los diferentes receptores para el aprendizaje en un asunto concreto, evitar desviar la atención, ayudar a evitar el cansancio y estimular el interés por la temática.
- El estudiante tiene la posibilidad de establecer su propio ritmo de trabajo de acuerdo con la rapidez con que asimila los contenidos y sus intereses. Puede establecer un orden personalizado al navegar entre los diferentes aspectos que presenta este medio, escogiendo cual asunto estudiará, participando así activamente en el proceso de adquisición de conocimientos. Es obvio que este nivel de libertad está condicionado por la lógica del contenido y del conocimiento.
- Las diapositivas, incluyen en muchos casos otros asuntos de interés, como aplicaciones tecnológicas, cuestiones históricas, reseñas y fotos de científicos, etc. que además de elevar el conocimiento general del asunto, intentan ayudar a despertar intereses cognoscitivos e investigativos.

5. Conclusiones

- Se realizó una exploración teórica de las características de las Tecnologías de Información y Comunicación sustentadas en el uso de la computación, sus diferentes formas, y en especial la estructura de una multimedia; el uso de las TIC en el proceso de enseñanza-aprendizaje; elementos didácticos y psicopedagógicos para sustentar la elaboración del medio.
- Se diagnosticó la situación en cuanto al uso de medios informáticos en el proceso de enseñanza-aprendizaje de Física II para las carreras de ingeniería en la UHo.
- Se elaboraron seis materiales multimedia de seis temas de electromagnetismo, conteniendo ilustraciones, cuadros resúmenes, modelos animados, ampliación en las temas objeto de estudio, etc. El medio tiene interactividad y permite al estudiante dirigir por sí mismo el ritmo de navegación y aprendizaje. Fue elaborado teniendo en cuenta principios didácticos y psicopedagógicos.

- Se valoró el material didáctico multimedia en actividades metodológicas del departamento de Física de la UHo. Ha sido empleado por los profesores en el desarrollo de actividades docentes, fundamentalmente en conferencias. Los estudiantes usan el material en el estudio independiente.
- El uso de la multimedia se ha extendido a otras especialidades, además de aquella para la que fue concebido y ha estimulado a profesores a elaborar medios de este tipo.
- El Dpto. de Física de la UHo intensifica el uso de las TIC concibiendo una importancia central en esta actividad el trabajo que aquí se expone.

Referencias

[1] Carina S. González, César A. Collazos y Roberto García. "Desafío en el diseño de MOOCs: incorporación de aspectos para la colaboración y la gamificación". En: *Revista de Educación a Distancia* 48 (2016).

[2] Manuel Esteban y Miguel Zapata Ros. "Estrategias de aprendizaje y eLearning. Un apunte para la fundamentación del diseño educativo en los entornos virtuales de aprendizaje. Consideraciones para la reflexión y el debate. Introducción al estudio de las estrategias y estilos de aprendizaje". En: *Revista de educación a distancia* 19 (2008).

[3] José Miguel Correa Gorospe y col. "Formación del profesorado, tecnología educativa e identidad docente digital". En: *RELATEC: Revista Latinoamericana de Tecnología Educativa* 14.1 (2015), págs. 45-56.

[4] María Dolores Afonso Suárez. "Aportaciones al desarrollo de una ingeniería de contenidos docentes". PhD Thesis. 2013.

[5] Miguel Ángel Marzal García-Quismondo, Francisco Javier Calzada Prado y Marina Vianello Osti. "Criterios para la evaluación de la usabilidad de los recursos educativos virtuales: un análisis desde la alfabetización en información". En: (2008).

[6] Viviana Berrocal Carvajal. "Consideraciones para el uso de simulaciones en entornos virtuales para el aprendizaje de las estrategias de programación de computadoras". En: *Innovaciones educativas* 11.16 (2009), pág. 7.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 33-42 ISSN 2550-6730

Recibido: 15/02/2020
Aceptado: 06/03/2020

Estudio de factibilidad de un sistema de bajo costo para la monitorización del tráfico de vehículos por medio de la detección de dispositivos WiFi.

Fabricio Javier Santana Campoverde [1] David Fernando Zambrano Montenegro [1]

[1]Universidad Tecnica de Manabi, Ecuador

RESUMEN
El presente trabajo de investigación tiene como propósito evaluar la factibilidad de un sistema de bajo coste para la estimación del comportamiento del tráfico vehicular por medio de la identificación de dispositivos wifi a bordo de los vehículos. Se pretende que este trabajo tenga proyección a que se pueda implementar a nivel de la ciudad si se logran los resultados esperados, debido a los bajos costos en relación a otros métodos comúnmente empleados en las diferentes ciudades del Ecuador. Para ello se estableció como escenario de evaluación a la Universidad Técnica de Manabí, en la misma se desplegó un sistema de monitorización de entrada y salida de dispositivos móviles mediante WiFi. Este sistema permitió captar información que determinó la posibilidad de utilizar esta técnica para la estimación de la movilidad en el acceso a la universidad. En este trabajo se realizó un conjunto de pruebas, que no pueden considerarse en rigor como concluyentes, sin embargo, en sentido general se aprecia correspondencia en el comportamiento de entradas y salidas de personal de la Universidad Técnica de Manabí.
Palabras-clave: WiFi; sistema; tráfico vehicular; movilidad; monitorización.

ABSTRACT
The purpose of this research work is to evaluate the feasibility of a low-cost system for estimating the behavior of vehicular traffic through the identification of Wi-Fi devices on board vehicles. It is intended that this work has a projection that can be implemented at the city level if the expected results are achieved, due to the low costs in relation to other methods commonly used in the different cities of Ecuador. For this purpose, the Technical University of Manabí was established as an evaluation scenario, in which a system for monitoring the entry and exit of mobile devices via WiFi was deployed. This system allowed to capture information that determined the possibility of using this technique for the estimation of mobility in university access. In this work, a set of tests was carried out, which cannot be considered strictly as conclusive, however, in general, correspondence can be seen in the behavior of staff entries and exits of the Technical University of Manabí.
KEYWORDS: WiFi; system; Vehicular traffic; mobility; monitoring

1. Introducción

En el Ecuador son conocidos los problemas de congestión vehicular que se presentan en ciudades grandes y medianas. Específicamente en la ciudad de Portoviejo esta situación ha ido ganando relevancia y se ha constituido en la actualidad como uno de los problemas en los que se hace necesario el empleo de las técnicas más pertinentes de obtención y análisis de datos para poder tomar las decisiones más adecuadas. En este contexto la evaluación del tráfico vehicular constituye actualmente un aspecto de especial importancia en el propósito de gestionar de una mejor manera la movilidad en ciudades y carreteras, a través de la captación, análisis y difusión de datos e información elaborada que puedan contribuir al diagnóstico de la situación actual, realizar estimaciones y extraer comportamientos y tendencias para la planificación de desarrollos futuros o un mejor aprovechamiento de los recursos disponibles.

Esto puede verse tanto desde la óptica de las autoridades en la toma de decisiones relacionadas con el tráfico o de los propios usuarios de las vías, que pueden estar entonces en una condición más informada para la elección de las mejores rutas. De lograr resultados positivos es de esperar la disminución de costos de operación, prevención o mitigación de atascos, con el consiguiente ahorro de tiempo y energía.

Con este fin es muy importante poder contar con un sistema que permita la monitorización del tráfico vehicular para proveer de datos a los sistemas encargados de extraer la información relevante para la toma de decisiones. Por otro lado, estos sistemas, más allá de su utilidad, traen consigo la necesidad de contar con un equipamiento que suele ser en general muy caro, o requieren de acciones de intervención en la vía pública que pueden tener impacto en su funcionamiento y seguridad.

Algunos trabajos de investigación realizados en diferentes países, sobre todo los desarrollados, han mostrado la posibilidad de emplear la identificación de los dispositivos wifi, que se encuentran a bordo de los vehículos, como una alternativa barata y bastante eficiente en la estimación de los flujos de tráfico en las vías de transporte terrestre.

Tradicionalmente se han venido utilizando diversos sistemas con el objetivo de detectar el paso y en algunos casos la identificación de vehículos en lugares seleccionados de la vía pública.

Entre los más conocidos se encuentran los llamados sistemas intrusivos entre los que se encuentran los dispositivos de tubos neumáticos, lazos inductivos, sensores piezoeléctricos y sensores magnéticos, mientras que como no intrusivos pueden mencionarse los sensores infrarrojos, radares de microondas, arreglos de sensores acústicos y sistemas de procesamiento de vídeo que pueden incluir el reconocimiento de caracteres para la identificación de matrículas [1][2] entre otros. Como se ve no todos permiten estimar rutas de vehículos, teniendo en cuenta que no son capaces de identificarlos, lo cual puede incidir de manera significativa en un aumento de la complejidad y el costo de los sistemas a desplegar.

Más recientemente se han comenzado a utilizar sistemas que utilizan las señales de dispositivos wifi que se encuentren a bordo de los vehículos, tanto aquellos que están incorporados a los equipos que forman parte de las prestaciones del vehículo como los que llevan los pasajeros de este. Este enfoque representa una alternativa mucho más económica y sencilla para la estimación no sólo de la cantidad de vehículos que están pasando por el lugar donde se ubica el dispositivo de captación, sino que también ofrece la posibilidad de estimar rutas, en dependencia de una adecuada distribución de estos captadores.

Es común utilizar con este fin la identificación de las direcciones MAC que con carácter único tiene cada dispositivo. Este enfoque ha sido probado con éxito por investigadores en varios países, y se conoce de trabajos publicados tanto acerca de la extracción de información a partir de los datos colectados como de la evaluación de la efectividad del sistema en la estimación del tráfico vehicular.

Se ha investigado en la evaluación de la validez de este enfoque como sistema de captación del tráfico o en su comparación con otros sistemas más tradicionales cuya eficacia ha sido establecida con anterioridad [3][4]. Igualmente se conoce del desarrollo de sistemas que usan esta tecnología que han sido utilizados como una manera de estimar las condiciones y variabilidad de tráfico urbano o de autopistas de Estados Unidos, Australia y España [5][6][7].

Desde hace algún tiempo se han venido desarrollando en la Universidad de Granada, en España, proyectos para la monitorización del tráfico vehicular mediante sistemas de bajo coste de identificación de señales wifi de los dispositivos a bordo de los vehículos, el almacenamiento de los datos en infraestructura de nube y la aplicación de técnicas de inteligencia computacional a la extracción de la información relevante

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 33-42 ISSN 2550-6730

de estos[8][9].
Existen relaciones de trabajo de varios años de docentes de la Facultad de Ciencias Informáticas de la UTM (FCI-UTM) con miembros del grupo de investigación de la universidad de Granada que han estado desarrollando estos proyectos y existe interés mutuo en la transferencia del conocimiento y las tecnologías involucradas para su implementación en proyectos en el Ecuador.
Este es un grupo de investigación consolidado, de una universidad que es primera de España en el ranking de Taiwán en el área de la informática, que en la actualidad ocupa una posición de relevancia entre los grupos de investigación dedicados a la computación evolutiva y que ha participado en una cantidad considerable de proyectos de investigación en esta área.
La realización de un proyecto de esta naturaleza en la UTM va más allá de los resultados directos de la investigación y de los beneficios de su aplicación a la solución de problemas de importancia en el entorno, como es el caso de la gestión del tráfico vehicular. Es importante tener en cuenta que el trabajo de investigación desarrollado con la participación de los profesores de la universidad de Granada necesariamente debe tener un impacto en la formación de capacidades de investigación en los docentes, la publicación de resultados científicos y la asimilación de técnicas de avanzada en el campo de la informática, mejorando asimismo la visibilidad de la facultad de ciencias informáticas y de la UTM a nivel internacional.

2. Materiales y Métodos

El siguiente trabajo de investigación tiene como objetivo la estimación del comportamiento del tráfico vehicular por medio de la identificación de dispositivos wifi a bordo de los vehículos dentro de la Universidad Técnica de Manabí como proyecto piloto, con proyección a que se pueda implementar un macro proyecto a nivel de la ciudad si se logran los resultados esperados, debido a los bajos costos a relación a otros métodos comúnmente empleados en las diferentes ciudades del Ecuador, con esta tecnología permitiría cubrir zonas de mucho tráfico pudiendo así contabilizar el número de vehículos que pasan en un sector y saber las rutas que tome a lo largo de su camino, tanto al ir a su destino y el retorno del mismo, pudiendo estimar inclusive el tiempo que se demore en llegar de un sector a otro, pudiendo así estimar las horas y los lugares donde se formen colapsos vehiculares para que las autoridades de control puedan buscar soluciones que permitan mejorar el tráfico en las carreteras.

2.1. Equipamiento necesario para la captación de señales wifi.

El equipamiento que se utilizó en este trabajo de titulación fue 2 tarjetas de red inalámbricas Usb Adp Wireless High Gain Tp-link Tl-wn722n 150mbps para la captación de las señales Wifi de teléfonos celulares que van al interior de un vehículo que circulen cerca de los puntos de captación instalados en sectores estratégicos dentro de la universidad en donde el fluido vehicular es muy concurrido diariamente, 2 computadores Raspberry Pi 3 modelo B para el procesamiento de los datos y almacenamiento en la nube.
El Raspberry Pi 3 B es un computador moderno de poca capacidad comparado a un computador de escritorio o portátil, pero muy útil para poder emplearlo en proyectos académicos con fines científicos, se usa por la gran ventaja por su pequeño tamaño y su bajo costo.
A nivel mundial se han realizado experimentos tecnológicos muy interesantes de los cuales se han basado en buscar soluciones a problemáticas tales como: Capturas de imágenes por medio de cámaras, técnica de reconocimiento de voz, sistema de alarma contra incendios, ayuda visual por medio de sensores para personas con discapacidad, entre otros. Como material adicional se utilizó cable usb para conectar la tarjeta de red inalámbrica y la Raspberry Pi y dos cajas de plástico para brindar seguridad y protección a los equipos.

Figura 1: Cajas de seguridad y protección de equipo

2.2. Despliegue del sistema piloto en lugares seleccionados dentro de la Universidad Técnica de Manabí.

El sistema piloto se lo implementó en la provincia de Manabí, cantón Portoviejo, parroquia "12 de marzo" sector Av. José María Urbina y calle Che Guevara, en las facultades, departamentos y áreas de la Universidad Técnica de Manabí. El primer punto de captación se lo instaló en la puerta de acceso vehicular número dos de la UTM, específicamente en la caseta donde se reguarda el personal de vigilancia de la institución. El segundo punto de captación se implementó en un poste utilizado para tendido eléctrico ubicado en la Facultad de Filosofía Letras y Ciencias de la Educación. En la figura 2 se muestra en detalle la ubicación de los equipos de captación.

Figura 2: Puerta de acceso vehicular N°2

En el interior de la garita se instaló el computador Raspberry Pi 3 modelo B en una de las paredes de la

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 33-42 ISSN 2550-6730

caseta muy cerca del techo falso lo que permitió la conexión mediante cable USB con la tarjeta de red inalámbrica ubicada en el exterior de la garita. El segundo punto de captación se instaló en una caja de plástico para la protección de la Raspberry Pi y la antena inalámbrica USB, luego se implementó en el poste de tendido eléctrico. En la figura 3 se muestra detalles de la instalación de los equipos.
El primer punto de captación identificado como R1 posee las siguientes coordenadas geográficas: Latitud: 1° 2'45.63"S, Longitud: 80°27'18.62.°, Alcance: 302m, El segundo punto de captación identificado como R2 tiene una Latitud: 1° 2'43.42"S, Longitud: 80°27'15.45.°, Alcance: 302m. La distancia entre los dos puntos de captación de datos R1 y R2 es de 131 metros con una elevación de terreno aproximada de 53 metros. Los datos se obtuvieron mediante la herramienta Google Earth, misma que permitió establecer la ubicación de los puntos de captación y obtener las coordenadas geográficas, además mostró como resultado la distancia entre los dos puntos de captación y la elevación del terreno que existe entre los puntos.

2.3. Almacenar los datos en servicios de nube que permitan su acceso distribuido con fines de procesamiento y publicación.

Para almacenar los datos en la nube de manera automática se elaboró un conjunto de scripts que permitió la obtención fiable de los tiempos de acceso de cada uno de los dispositivos que circularon en el área aledaña a los puntos de captación. La configuración se realizó de manera tal que los datos captados fueran subidos directamente a una unidad de almacenamiento de Google Drive, disponibles en formato texto en archivos diarios por cada una de las estaciones de trabajo.

2.4. Configuración de la Raspberry Pi

Para almacenar datos en la nube se realizó la configuración de la tarjeta de red inalámbrica USB conectada al computador Raspberry Pi activando la opción de modo monitor, se utilizó la herramienta Airodump-ng, la cual se encarga de captar el tráfico de red del entorno inalámbrico, este algoritmo se utiliza para con la finalidad de capturar las direcciones MAC de los dispositivos celulares que van a bordo de los vehículos, con la particularidad que los dispositivos móviles deben de tener encendido el Wireless para qué pueda estos puedan hacer el petitorio de red a los Access Point.
Los datos captados por airodump son procesados y almacenados en la carpeta de salvas, de forma que sólo suba al drive de google la información ya filtrada, se eliminó columnas con información no deseada (por ej. redes almacenadas en los dispositivos móviles). Luego se procedió a actualizar ficheros en la Raspberry pi cada una hora. Es importante mencionar que para no perder datos durante la salva se inicia una nueva instancia de airodump antes de detener la que se está ejecutando (puede ser usando dos ficheros 1.csv y 2.csv alternando). Se determinó el formato de nombre de fichero diario en google drive: rXXXaaaammdd.csv, por ejemplo, la raspberry pi 1 el día 22 de octubre de 2016 su nombre es: r001pi20161022.csv. Los ficheros de cada raspberry están en una carpeta diferente en el drive de google. En este lugar de almacenamiento se encuentra un fichero diario en el cual se adiciona cada salva nueva por concatenación del fichero definitivo de ese día con el nuevo fichero subido.

2.5. API de google

Se logró unir los ficheros de una estación en uno solo sin la hora del día y envió a una carpeta y borró el fichero con la hora que se adicionó al fichero resumen del día. Este proceso se ejecutó cada 20 minutos, su función es revisar si hay algún fichero en el drive. Si existe, busca la carpeta de esa estación, dentro de esa carpeta busca el fichero de ese día, si no existe lo crea, y se hace append y borra el fichero del drive. El archivo con formato csv contiene los datos captados por el sistema, entre los datos captados se muestra los siguientes: dirección MAC del dispositivo, dirección IP, canal, tipo de autenticación, cifrado,

número de paquetes, beacons, velocidad y nombre de la red. Estos archivos con formato csv se encuentran almacenados en Google Drive en la cuenta rgb.proywifi@gmail.com que fue creada para cumplir con el objetivo planteado.

2.6. Scripts para la captación y procesamiento de los datos en la nube.

A continuación, se muestra en detalle los scripts creados utilizando el cron de Linux para la captación de datos, ordenamiento y procesamiento de los ficheros y mecanismos para subir la información al google drive. Los scripts se ejecutan de forma automática en la fecha y hora establecida en el código.
config.txt. - Este archivo ejecuta airodump en el minuto 48 de cada hora, y sube la información a google drive en el minuto 50 de cada hora.
Config2.txt. - Este archivo tiene almacenado el número 2 y se utiliza para concatenar el fichero definitivo de ese día con el nuevo fichero subido.
Encripting. - La MAC se encripta con SHA512 en el momento en que se va a mover el fichero de datos a la carpeta de datos.
Monitwifi. - Es el servicio que está en la carpeta init.d del sistema operativo para que se ejecute cada vez que la raspberry inicializa.
Microntab0.- En el minuto 48 de cada hora ejecuta a prueba2.sh; En el minuto 50 de cada hora ejecuta a prueba3.sh
Prueba2.- Arranca o restablece el airodump encripta la mac en el miunto 48 de cada hora, mueve el archivo con formato csv de la estación a la carpeta de subida con el nombre codificado con fecha-hora-nombre de la estacion.csv
Prueba 3.- En el minuto 50 de cada hora recorre la carpeta de subida y todos los ficheros con formato csv de esa carpeta son subidos al google drive.

3. Resultados

El análisis de la información recolectada, se orientó sobre todo a la determinación de la efectividad del sistema de captación en cuanto a su cobertura, precisión y exactitud, entre otros aspectos, permitió conocer en qué medida esta tecnología es capaz de detectar de una manera fiable los vehículos que circulan en su área de captación.

Se elaboró programas en Matlab para el procesamiento y análisis de la información captada presente en Google Drive, lo que permitió conocer el comportamiento de la entrada y salida de dispositivos móviles en la Universidad Técnica de Manabí, lo que confirmó la posibilidad de utilizar esta técnica en la estimación de la movilidad en el acceso a la universidad.

En la figura 3, se muestra la entrada y salida de los dispositivos captados, el eje X representa la hora de entrada con barras de color azul y la hora de salida con barras de color rojo. El eje Y representa la cantidad de dispositivos que fueron captados por el sistema.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 33-42 ISSN 2550-6730

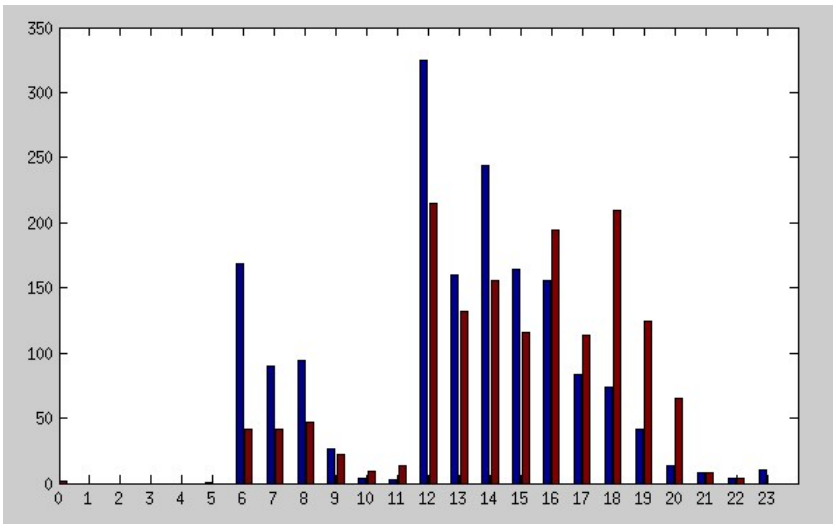

Figura 3: Cantidad de dispositivos captados

La gráfica muestra que la cantidad máximo de dispositivos que ingresó fue de 320 y la cantidad de dispositivos que salieron fue de 220, estos resultados se dieron en horario del medio día, específicamente a las 12H00. A las 14H00 se registra el segundo ingreso más alto con 250 dispositivos ingresados y 150 que salieron. Otro horario en el que se muestra una cantidad importante de ingreso de dispositivos fue a las 06H00 con 160. Entre las 16H00 y 19H00 se registra un aproximado de 250 dispositivos que salieron de la Universidad Técnica de Manabí.

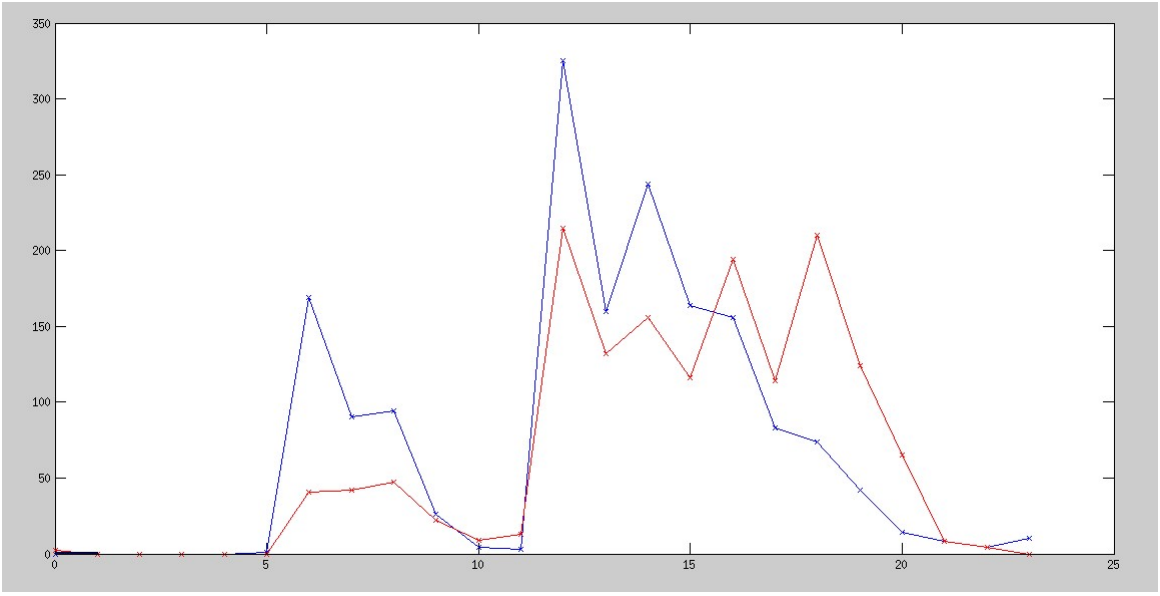

Figura 4: Representación lineal de dispositivos captados

La figura 4, muestra los resultados de forma lineal y con puntos, la línea azul representa la cantidad de dispositivos que ingresa y la línea roja la cantidad que sale. El eje X representa el horario el cual fue

establecido desde 0 hasta 25 tomando saltos de 5 horas, el eje Y representa el número de dispositivos entre 0 hasta 350 tomando saltos de 50.

4. Discusión

Se considera que los objetivos planteados al inicio de este trabajo de investigación fueron cumplidos en sus aspectos más esenciales por tanto puede concluir que la investigación demostró la factibilidad de realizar un sistema WIFI para la monitorización de entrada y salida de dispositivos móviles en la Universidad Técnica de Manabí, a través de este sistema se logró captar, procesar y analizar información que determinó la posibilidad de utilizar esta técnica para la estimación de la movilidad en el acceso a la universidad.

La implementación de 2 puntos de captación autónomos sobre un dispositivo embebido Raspberry Pi permitió la obtención fiable de los tiempos de acceso de cada uno de los dispositivos que circularon en el área aledaña a los puntos de captación.

Se utilizó el programa Matlab para el procesamiento y análisis de la información almacenada en Google Drive, lo que permitió conocer el comportamiento de la entrada y salida de dispositivos móviles en la Universidad Técnica de Manabí y se mostró los resultados mediante gráficos generados por esta aplicación.

En este trabajo se realizó un conjunto de pruebas, que no pueden considerarse en rigor como concluyentes, sin embargo, en sentido general se aprecia correspondencia en el comportamiento de entradas y salidas de personal de la Universidad Técnica de Manabí.

Este trabajo debería tener una continuación en el uso de técnicas estadísticas y de inteligencia artificial que permitan la identificación de cada vehículo a partir del análisis conjunto de la movilidad de sus dispositivos a bordo. En un futuro cercano se considere realizar pruebas más exhaustivas en puntos seleccionados de la ciudad de Portoviejo, para realizar estas pruebas está pendiente la autorización correspondiente de las autoridades que controlan el espectro radioeléctrico en el país.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 33-42 ISSN 2550-6730

Referencias

[1] Luz Elena Y. Mimbela y Lawrence A. Klein. "Summary of vehicle detection and surveillance technologies used in intelligent transportation systems". En: (2000).

[2] L. Marzan y col. "Digital Image Processing Applied To Traffic". En: *1994* 74 ().

[3] Yegor Malinovskiy y col. *Field experiments on bluetooth-based travel time data collection*. Inf. téc. 2010.

[4] Chris Bachmann y col. "A comparative assessment of multi-sensor data fusion techniques for freeway traffic speed estimation using microsimulation modeling". En: *Transportation research part C: emerging technologies* 26 (2013), págs. 33-48.

[5] Le Minh Kieu, Ashish Bhaskar y Edward Chung. "Bus and car travel time on urban networks: integrating bluetooth and bus vehicle identification data". En: (2012).

[6] Maria Martchouk, Fred Mannering y Darcy Bullock. "Analysis of freeway travel time variability using Bluetooth detection". En: *Journal of transportation engineering* 137.10 (2010), págs. 697-704.

[7] Mireia Peira Bayo. "Estudio de una solución para la localización de autobuses en cocheras de TMB". En: (2009).

[8] P. A. Castillo y col. "Sistema de información autónomo y de bajo coste para conocer el estado de las carreteras en tiempo real". En: *Congreso Español de Informática*. 2010.

[9] V. M. Rivas y col. "Predicción de tráfico mediante co-evolución de Redes Neuronales de Funciones de Base Radial y selección de variables de entrada". En: *Ix Congreso Espanol De Metaheurısticas, Algoritmos Evolutivos Y Bioinspirados (MAEB 2013)*. Vol. 1. 2013, págs. 782-791.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 42-51 ISSN 2550-6730

Recibido: 02/04/2020
Aceptado: 15/04/2020

La importancia de la autenticación multifactor para el usuario final en un entorno financiero.

Alex Mendoza Arteaga [1] Francisco Bolaños Burgos [1] Cristhian Cedeño Sarmiento [1] Wilton Rafael Saltos Rivas [2]

[1]Universidad Espíritu Santo – Ecuador.,
[2]Universidad Técnica de Manabí – Ecuador.
alexmendoza@uees.edu.ec, fcobolanos@uees.edu.ec, cfcedeno@uees.edu.ec,
w.saltos@utm.edu.ec

RESUMEN
En la actualidad, encontrar sistemas de autenticación multifactor es común, en especial en los sitios web de las entidades financieras y las que se dedican al comercio electrónico, en el presente artículo se revisó apartados, reportes e informes para analizar la importancia de la autenticación multifactor para el usuario final en un entorno financiero. Para alcanzar este objetivo se analizan los ataques a los sistemas de autenticación, así como los métodos y su clasificación, también la forma óptima de implementar los sistemas de multifactor de autenticación considerando costo, complejidad e interacción con el usuario final. Por lo consiguiente se concluye, que el uso de los sistemas de multifactor de autentificación en los sitios web de las empresas dentro del entorno financiero, se convirtió en una necesidad para garantizar a sus clientes la seguridad de su información y evitar el robo de dinero.
Palabras-clave: Autenticación; Multifactor; doble factor; financiero.

ABSTRACT
Currently finding multifactor authentication systems is common in particular in the websites of financial institutions and those engaged in electronic commerce, in this article articles, reports and reports were reviewed to analyze the importance of multifactor authentication for the end user in a financial environment. To achieve this goal, we analyze attacks on authentication systems, as well as methods and their classification, as well as the optimal way to implement multifactor authentication systems considering cost, complexity and interaction with the end user. As a result, it is concluded that the use of multifactor authentication systems in companies' websites within the financial environment became a necessity to guarantee their clients the security of their information and avoid the theft of money.
KEYWORDS: Authentication; Multifactor; double factor; financial.

1. Introducción

Actualmente los principales ataques cibernéticos en el área financiera son los phishing y códigos maliciosos o malware, incluyendo ataques a bancas virtuales, dispositivos móviles y cajeros automáticos, información basada en las estadísticas y datos de [1], también en los informes de tendencias emitidos por [2] muestran que en el segundo trimestre del año el 46,23 % de los ataques de phishing son al sector financiero, distribuidos en los ámbitos de comercio electrónico con el 20,3 %, sistemas de pagos en línea 24,7 % y bancos con el 55,00 %, asimismo encontramos que del total de personas que han recibido ataques de malware, el 4,8 % esta relacionados con amenaza financiera. De igual manera, ESET (2016) en los datos obtenidos por sus productos en Latinoamérica muestran que los primeros lugares de ataques cibernéticos son los relacionados con malware con el 40 % y el phishing 16 %, independientemente del tipo de empresas analizadas.

Con respecto a las técnicas de ataque mencionadas, [3][4] señalan que el phishing se refiere a un ataque mediante el cual se engaña a la víctima por medio de un correo electrónico, haciéndole creer que ha sido enviado por algún banco o entidad financiera del cual es cliente, incitándolo a que, mediante mensajes , el usuario acceda a sitios web falsos, provocando que divulguen su información personal o en otros casos instalen un malware en el equipo, lo que permite al atacante espiar las comunicaciones de los sitios web que visita, obteniendo así información de las cuentas personales.

Según [5], la propagación de los fraudes a distancias, mediante el uso de plataformas tecnológicas, ha generado mayor atención en los procesos de autenticación e identificación. [6][7] mencionan que el proceso dominante en el control de acceso, es el uso de contraseñas; este proceso fue tan exitoso, que la mayoría de sitios web empezaron a usarlo y se convirtió en blanco de una enorme variedad de ataques a cuentas de correo electrónicos, sistemas bancarios, médicos y redes sociales. [8] indica que las contraseñas no son nada seguras y expresa que por más extensa y compleja que sea, los criminales cibernéticos pueden robarla tanto mediante un malware, como por medio de phishing.

Para reducir este tipo de ataques, un solo factor de autenticación no es seguro, por lo que en la actualidad la autenticación multifactor es la tendencia para asegurar que los usuarios sean legítimos[9]. El principal objetivo de este artículo es demostrar al usuario final la importancia de la autenticación multifactor para reducir el riesgo de robo de información y dinero con una revisión de seis métodos de autenticación y su clasificación.

2. Marco Teórico

Ataques Informáticos

Según [10] un ataque informático radica en aprovechar la vulnerabilidad en el hardware, en el software, e incluso en los usuarios que forman parte de un entorno informático con la finalidad de obtener un beneficio, la mayoría de veces de índole económico, causando un efecto negativo para las personas y empresas.

Los ataques informáticos más comunes al área financiera son el phishing y malware según estadística de[1][2], ESET (2015) y ESET (2016), en general para que estos ataques tengan el éxito deseado por los cibercriminales, son acompañados de otra técnica conocida como ingeniería social, que analiza el comportamiento humano para encontrar sus vulnerabilidades y llegar de esa forma a la información deseada [11][12]

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 42-51 ISSN 2550-6730

Códigos Maliciosos (Malware)

El malware es un término que se le da a los códigos o programas maliciosos que afectan al computador, convirtiéndose actualmente en una de las principales amenazas para los sistemas informáticos.

Con el paso del tiempo, el malware se ha vuelto cada vez más sofisticado, al punto en que varias soluciones de prevención como los sistemas antispyware y antivirus se ven superadas, lo que permite que los virus aprovechen estas ventajas de la tecnología para ser rápidos, nocivos y sutiles y engañar así a sus víctimas[11].

La ventaja que posee el malware con otras sofisticadas técnicas de ataque, es que en la mayoría de las ocasiones aprovecha la inocencia de las personas; es decir, los creadores de malware utilizan técnicas como ingeniería social para engañar y abusar de sus víctimas, aunque hay que tener en cuenta que los cibercriminales desarrollan los malware a margen de la tecnología y evolucionan de manera permanente [10].

Phishing

Hoy por hoy existen muchos métodos de atentar contra la seguridad de la información.

Dentro de las estafas cibernéticas encontramos como uno de los delitos más comunes el Phishing, delito que va acompañado de la ingeniería social para lograr su objetivo y adquirir información de forma fraudulenta [12].

[12][3][4] describen el phishing como el proceso mediante el cual el estafador se hace pasar por una empresa o persona de confianza y por medio de llamadas telefónicas o correos electrónicos intenta obtener los datos que desea. Cuando el estafador realiza estas comunicaciones, en la mayoría de los casos ha estudiado a su víctima mediante técnicas de ingeniería social.

Autenticación y Autorización

La autenticación es el mecanismo principal de un modelo estándar de seguridad, es importante diferenciar entre la autenticación y la autorización, siendo la autorización otro elemento importante en una estrategia de seguridad de la información. La autenticación prueba la identidad de un usuario, luego la autorización verifica los privilegios del usuario y que tenga los permisos correspondientes a los recursos o lugares donde se pretende acceder[13].

Multifactor de Autenticación

Actualmente, la autenticación de factor único, usuario y contraseñas, ya no se considera seguro en el mundo de Internet, especialmente en el sector financiero. Las contraseñas comunes que son en la mayoría de los casos las más usadas, como los nombres y la edad, son fácilmente descubiertas por los ataques con técnicas como diccionario y de fuerza bruta.[14] Sin tomar en cuenta que cuando los usuarios son víctimas de phishing y malware como indica [8], por más robusta y compleja que sea la contraseña son blanco fácil de los cibercriminales.

Los métodos de autenticación han evolucionado con el paso del tiempo, en la actualidad las tendencias se basan en autenticación multifactor para identificar a los usuarios de forma correcta. La técnica multifactor parte de combinar métodos de autenticación, llevándola más allá de un simple factor como un usuario y una contraseña[15][9]).

Métodos de autenticación

Para el presente artículo realizaremos una revisión de algunos métodos de autenticación, tomando en cuenta que toda forma de la misma se basa en la validación de uno de estos tres elementos: Algo que sabes, Algo que tienes, Algo que eres [15][16][17]. Algo que sabe, es un secreto que solo el usuario conoce, como una contraseña, que puede generarse en cualquier instante para el sistema de autenticación. Algo que tienes, es cualquier dispositivo físico que el usuario lo posea en el momento de la autenticación. Algo que eres es el análisis de algún rasgo físico o conducta sobre un usuario que normalmente nunca cambiará, también conocido como biometría humana [15][17].

Contraseña

El usuario y la contraseña es el método de autenticación más conocido y más utilizado en la mayoría de sitios web, se encuentra dentro del grupo del elemento algo que sabes, siendo su mayor defecto que el nivel de seguridad depende directamente del usuario final, la complejidad de la contraseña, siempre es escasa, y las contraseñas demasiado complejas conducen a los usuarios a aplicar estrategias no siempre correctas para recordarlas, como anotarlas en el teléfono celular, en un archivo de Excel en el computador y hasta en una nota pegada al monitor del ordenador, dentro de sus ventajas encontramos que es un método fácil de utilizar e implementar y de muy bajo costo [16][18][6].

One-Time Password(OTP)

Otro método del grupo del elemento algo que sabes es el OTP el cual asegura el uso de la contraseña, en efecto, con un sistema OTP el usuario posee una contraseña por un tiempo determinado y para un uso específico. Esta solución es usada en general para el proceso de autenticación de inicio para los accesos externos, los cuales se realizan mediante P/VPN[19].

Tarjeta inteligente

Pertenece al grupo del elemento algo que tiene, el uso de tarjetas inteligentes que es cada vez más frecuente, ya que suministran información específica a un usuario en distintos escenarios, como por ejemplos, en el comercio electrónico, control de acceso y en la actualidad algunos países la han incorporado como documento de identidad. Para que un sistema que utiliza tarjetas inteligentes trabaje, debe estar compuesto por dos componentes fundamentales, las tarjetas inteligentes y un dispositivo de interfaz, frecuentemente conocido como un lector. Las tarjetas inteligentes son de uso personal de los usuarios del sistema, por lo que debe ser transportada dentro de sus bienes personales[20][21][22].
Con el paso del tiempo las tarjetas inteligentes han ido evolucionando considerablemente, estas incluyen memoria que almacena la información que es pertinente a la interacción del usuario con el sistema. En un sistema de comercio electrónico, cada tarjeta inteligente puede contener el saldo de una cuenta, así como los detalles de las transacciones, en la actualidad las tarjetas inteligentes también incluyen microprocesadores, por lo cual mejora su flexibilidad, facilita el almacenamiento de los programas ejecutables y proporciona amplias funcionalidades [20][21][22].

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 42-51 ISSN 2550-6730

Token

Un token es otro de los métodos de autenticación del grupo del elemento algo que tiene, es un dispositivo electrónico que posee la autorización de un servicio computarizado para un usuario específico a fin de facilitar el proceso de autenticación. El token es el dispositivo de seguridad utilizado para firmar digitalmente y cifrar mensajes, es un nivel de seguridad alto, con el cual se puede acceder a servicios que demandan certificados digitales y por el cual el usuario que posee esta llave puede acceder. Este dispositivo combina las funcionalidades de una tarjeta inteligente y su lectora en un solo hardware, siendo de fácil uso y manipulación, el usuario lo puede trasladar a cualquier parte del mundo. Existe más de una clase de token, como los conocidos generadores de contraseñas dinámicas OTP y la que comúnmente denominamos tokens USB los cuales no solo permiten almacenar contraseñas y certificados, sino que también almacenan la identidad digital de la persona [23].

En conclusión y en el contexto de la autentificación electrónica, un token es un dispositivo de almacenamiento que contiene una llave secreta para ser utilizado en el proceso de autenticación, la información que posee el dispositivo es certificada por una entidad que valida la autenticidad del mismo [24].

Biometría

Biometría es la autentificación de un individuo por medio de sus características físicas: forma de su rostro, huellas dactilares, estructura y forma de su voz, patrón de iris y otras características únicas de cada ser vivo. También se puede considerar a la biometría como una ciencia que mide las propiedades físicas en los seres vivos, por lo tanto aprovechando las características únicas del cuerpo se crean los sistemas biométricos y con éstos se permite la identificación tecnológica de una persona automáticamente utilizando características físicas de sí mismo [25].
De esta manera los sistemas biométricos se caracterizan por el reconocimiento de patrones que identifican a las personas de una forma automática, a partir de su comportamiento o características físicas, excluyendo de esta a los sistemas no automáticos como los procedimientos y métodos utilizados en la medicina forense. Por lo tanto el reconocimiento biométrico consiste en almacenar, medir y comparar las características de una persona, y ya que la dimensión de la identificación biométrica es muy amplia, nos remitimos a uno de ellos: el reconocimiento facial [26][27].

Reconocimiento facial

El reconocimiento facial data del año 1871, año donde se realizó el primer intento de identificar a una persona comparando su rostro con un grupo de imágenes, más tarde en 1882, el criminólogo Alphonse Bertillon, de origen francés, usó un método que consistía en tomar medidas de todo los rastros posibles de la cara y con esto crear una base de datos de rasgos faciales, en resumidas cuentas el principio de reconocimiento facial parte en registrar las medidas de varios puntos característicos del rostro de un individuo, dado que en un rostro común se puede encontrar puntos significativos como: ojos, pupilas, boca, cejas entre otros. De manera que analizando y apoyándose en cada una de las distancias obtenidas de los puntos característicos del rostro se podía identificar caras iguales [28].
Por lo tanto, el reconocimiento facial pertenece al grupo del elemento algo que eres, el cual tiene la capacidad de reconocer a un individuo por sus características o rasgos faciales. En la actualidad existen algoritmos escritos en computadoras que se encargan de mapear los rasgos faciales de las personas y compararlas con bases de datos, realizándolo con alta precisión y con una respuesta rápida. Igualmente podemos decir que el reconocimiento facial parte de la detección del rostro, extraer las características y realizar el reconocimiento[29].
El rostro de los seres humanos nos brinda un sinnúmero de información proporcionada por rasgos característicos que ayudan a identificar y discernir de manera fácil a las personas, debido a que la cara contiene elementos que a su vez poseen sus propios rasgos característicos, como la nariz, boca, cejas,

orejas y que siempre se encuentran en las mismas posiciones dentro de la cara de cualquier ser humano, esto ayuda al desarrollo de sistemas de reconocimiento facial ya que podría comparar narices con narices, bocas con bocas y así sucesivamente hasta encontrar similitudes entre sí[30].

Huella dactilar

La autenticación por huella dactilar es otro método del grupo del elemento de algo que eres, se caracteriza por extraer particulares desde distintos sectores y ángulos de la yema del dedo y de guardarlas. Las huellas dactilares son imborrables a lo largo de la vida de un ser humano, pero en algunas situaciones, por eventos externos que producen lastimaduras y cicatrices pueden alterarlas. Se ha convertido en una de las tecnologías más empleadas y de las que se han desarrollado diferentes aplicaciones y dispositivos de bajo costo que permiten la implementación de la tecnología biométrica, como por ejemplo: en controles de accesos,control de asistencia y autenticación a sistemas computacionales.[31]

Una huella dactilar es la representación de la morfología superficial de la epidermis de un dedo, esta posee un conjunto de líneas que, en forma global, aparecen dispuestas en formas paralelas. Sin embargo, estas líneas se intersectan y a veces terminan en formas abruptas. Los puntos donde las líneas terminan o se bifurcan, se conocen como puntos característicos. Para concluir, para saber si dos huellas dactilares corresponden o no a una misma persona se realiza el procedimiento que comienza con la clasificación de la huella dactilar y se culmina con la comparación de los puntos característicos de ambas huellas.[32]

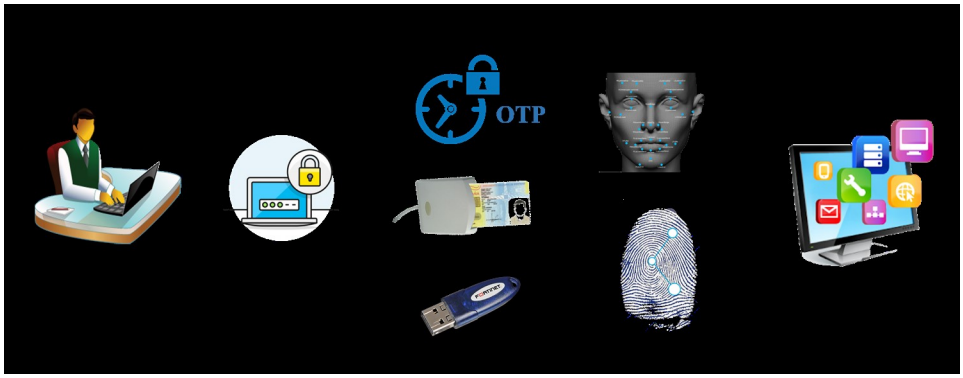

Figura 1: Factores de autenticación, según categoría.

3. Conclusiones, Limitaciones y Trabajos Futuros

Luego de la revisión de artículos, informes, foros relacionados a la autenticación, los métodos y clasificación, se puede evidenciar que la autenticación de factor simple es la que ha liderado los sistemas de autenticación en la mayoría de sitios web, usando el método de contraseña como único factor en la autentificación para identificar al usuario. Los reportes e informes de las marcas de antivirus indican alto índice de ataques mediante las técnicas conocidas como phishing y malware, evidenciando que las contraseñas son blanco fácil de los cibercriminales, especialmente en los usuarios de bancos y comercio electrónico. Otros autores afirman que la complejidad de la contraseña no garantiza que no pueda ser vulnerada, ya que en la actualidad los ataques se inclinan más a robar los datos con engaños, antes de intentar descifrar las contraseñas.

Con estas debilidades que la mayoría de empresas en el entorno financiero han encontrado, los desarrolladores e investigadores de los sistemas de autenticación luchan por implementar nuevas formas de garantizar que los usuarios no sean víctimas de fraudes cibernéticos y evitar así que su información y dinero sean robados. Actualmente la tendencia en la autenticación de usuario se basa en multifactores

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 42-51 ISSN 2550-6730

que no es más que un conjunto de factores de autenticación (figura 1), tomando en cuenta los elementos de la misma: algo que sabe, algo que tiene y algo que es, para crear sistemas de autenticación multifactor complejos, pero a su vez se busca que sea de fácil uso para el usuario final. Aunque se ha evidenciado que la contraseña, por sí sola, no es un método seguro de autenticación, los procesos de autenticación multifactor en la mayoría de los casos la sigue implementando acompañada de un segundo factor que por costos es un token o tarjeta inteligente u objeto físico que el usuario siempre lleva con él, y que pertenece a uno de los métodos del grupo del elemento algo que se tiene.

En la revisión literaria podemos encontrar que el método más seguro para garantizar la identidad de un usuario, es la biometría del grupo del elemento algo que es, este tercer elemento de la autenticación que es casi imposible de suplantar ya que se realiza la identificación mediante un rasgo físico o del comportamiento de un individuo. En el presente trabajo se analizó 2 métodos de autenticación biométrica, el reconocimiento facial y el reconocimiento por huella dactilar, pero el costo de la implementación en los sistemas de autenticación es muy elevado.

Las limitaciones de la investigación se encontraron en la aplicación del tercer grupo del elemento algo que es, ya que por el costo de aplicación y su complejidad no se evidencia su uso en los sitios web, al contrario, se utiliza en la mayoría de los casos en controles de accesos y de asistencia, sin embargo existen artículos de autenticaciones que emplean biometría pero en aplicaciones locales, por lo cual se propone realizar trabajos futuros orientados a la biometría como método de autenticación multifactor y realizar análisis técnicos de las combinaciones idóneas para generar sistemas de autenticación seguros económicos y de fácil uso para los usuarios finales.

Referencias

[1] Kasperski. *Financial cyber threats in 2014: things changed | Securelist*. 2014. URL: https://securelist.com/financial-cyber-threats-in-2014-things-changed/68720/ (visitado 05-05-2020).

[2] Kasperski y Telefonica. *Ciberamenazas Sector Financiero Q2 2016*. es-ES. 2016. URL: https://www.elevenpaths.com/es/ciberamenazas-sector-financiero-q2-2016/ (visitado 05-05-2020).

[3] Jason Hong. "The state of phishing attacks". En: *Communications of the ACM* 55.1 (2012), págs. 74-81.

[4] Jason Milletary y CERT Coordination Center. "Technical trends in phishing attacks". En: *Retrieved December* 1.2007 (2005), págs. 3-3.

[5] Luis Gerardo Gabaldón y Wílmer Pereira. "Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico". En: *Sociologias* 20 (2008), págs. 164-190.

[6] Dinei Florêncio, Cormac Herley y Baris Coskun. "Do strong web passwords accomplish anything?" En: *HotSec* 7.6 (2007), pág. 159.

[7] L. C. F. Araújo y col. "Autentificación personal por dinámica de tecleo basada en lógica difusa". En: *IEEE LATIN AMERICA TRANSACTIONS* 2.1 (2004), pág. 69.

[8] C. Alonso. *Un informático en el lado del mal*. Obtenido de http://www. elladodelmal. com/2017/04/publicada-owasp-top-ten ...

[9] Abhijit Kumar Nag y Dipankar Dasgupta. "An adaptive approach for continuous multi-factor authentication in an identity eco-system". En: *Proceedings of the 9th Annual Cyber and Information Security Research Conference*. 2014, págs. 65-68.

[10] Jorge Mieres. "Ataques informáticos: Debilidades de seguridad comúnmente explotadas". En: *ene-2009* (2009).

[11] Luis Fernando Fuentes Serrano. "Malware: una amenaza de Internet". En: (2008).

[12] Milagros Infante Montero. "Criptografía y psicología de la contraseña: generando una contraseña fuerte para diferentes servicios". En: *Apuntes de Ciencia & Sociedad* 3.1 (2013).

[13] Fatima Moumtadi y Luis Alfonso García Vázquez. "Autenticación multifactor con el uso de un sensor kinect". En: *ITECKNE: Innovación e Investigación en Ingeniería* 13.1 (2016), págs. 23-35.

[14] Fadi Aloul, Syed Zahidi y Wassim El-Hajj. "Two factor authentication using mobile phones". En: *2009 IEEE/ACS International Conference on Computer Systems and Applications*. IEEE, 2009, págs. 641-644.

[15] Hisham Al-Assam, Harin Sellahewa y Sabah Jassim. "Multi-factor biometrics for authentication: A false sense of security". En: *Proceedings of the 12th ACM Workshop on Multimedia and Security*. 2010, págs. 81-88.

[16] Mark Burnett. *Perfect password: Selection, protection, authentication*. Elsevier, 2006.

[17] Igor Ruiz-Agundez y Pablo G. Bringas. "Service authentication via electronic identification cards: voip service authentication through the DNIe". En: *2012 Annual SRII Global Conference*. IEEE, 2012, págs. 602-607.

[18] Niklas Auerbach. "Anonymous digital identity in e-government". PhD Thesis. University of Zurich, 2004.

[19] Neil Haller y col. "A one-time password system". En: *Network Working Group Request for Comments* 2289 (1998).

[20] William Reid Carlisle y col. "Smart card with multiple charge accounts and product item tables designating the account to debit". Jul. de 1997.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 42-51 ISSN 2550-6730

[21] Raúl Sánchez Reillo. "Mecanismos de autenticación biométrica mediante tarjeta inteligente". En: *Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingenieros de Telecomunicación* (2000).

[22] Jean-Marc Sarat. *Smart card which operates with the USB protocol*. Google Patents, jun. de 2003.

[23] Keitling Daysi Salinas Hinojosa. "TOKENS DE SEGURIDAD". En: *Revista de Información, Tecnología y Sociedad* (2013), pág. 59.

[24] William Burr, Donna Dodson y W. Polk. *Electronic authentication guideline*. Inf. téc. National Institute of Standards y Technology, 2004.

[25] Javier Areitio Bertolín y María Teresa Areitio Bertolín. "Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación". En: *Revista española de electrónica* 630 (2007), págs. 52-67.

[26] Virginia Espinosa Duró. "Evaluación de sistemas de reconocimiento biométrico". En: *Departamento de Electrónica y Automática. Escuela Universitaria Politécnica de Mataró* (2001).

[27] Ana Belén Moreno Díaz. "Reconocimiento facial automático mediante técnicas de visión tridimensional". PhD Thesis. Informatica, 2004.

[28] Maya Binetskaya. "Reconocimiento Facial en el ámbito Forense". B.S. thesis. 2013.

[29] Nicolas Lopez Perez, JJ Toro Agudelo y CIENCIAS DE LA COMPUTACION. "Técnicas de biometría basadas en patrones faciales del ser humano". PhD Thesis. Universidad Tecnológica de Pereira. Facultad de Ingenierías Eléctrica . . ., 2012.

[30] Javier Eslava Ríos. "Reconocimiento facial en tiempo real". B.S. thesis. 2013.

[31] José I. Carri y col. "Reconocimiento biométrico en aplicaciones de E-Government". En: *Congreso Argentino de Ciencias de la Computación*. Vol. 13. 2007.

[32] A. Arrieta y col. "Gestión y Reconocimiento Óptico de los Puntos Característicos de Imágenes de Huellas Dactilares". En: *Universidad de Salamanca* (2016).

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 64-77 ISSN 2550-6730

Recibido: 02/04/2020
Aceptado: 12/05/2020

Estudio exploratorio de la seguridad del DNI electrónico para su aplicación en Ecuador

Cristhian Cedeño Sarmiento [1] Francisco Bolaños Burgos [1] Alex Gregorio Mendoza Arteaga [1] Wilton Rafael Saltos Rivas [2]

[1]Universidad Espíritu Santo – Ecuador.
[1]Universidad Técnica de Manabí – Ecuador

cfcedeno@uees.edu.ec, fcobolanos@uees.edu.ec, alexmendoza@uees.edu.ec, w.saltos@utm.edu.ec

RESUMEN
En la actualidad la necesidad de contar con un dispositivo de identificación electrónica seguro que permita identificar y autenticar a los ciudadanos en actividades en línea es primordial, más aún en países que se encuentran implementando políticas de gobierno electrónico en su población y ante eventos diarios de ataques de suplantación de identidad en línea. En el presente artículo de revisión se realiza un análisis de la seguridad que existe en la implementación del documento nacional de identificación electrónico (DNIe) en España, las versiones que ha tenido el dispositivo, la tecnología que posee en la actualidad, la estructura interna, los tipos de certificados digitales de seguridad que almacena el chip criptográfico, la infraestructura de clave pública que soporta su funcionamiento y los casos de usos que se han propuesto para el dispositivo. Adicional se incluye una revisión de países que implementan dispositivos de identificación electrónica en ambientes de gobierno electrónico para sus ciudadanos, las posibles debilidades presentadas en este tipo de tarjetas criptográficas así como las contramedidas definidas por autores reconocidos en ambientes de ataques de canal lateral, por último se presenta una revisión de las instituciones públicas y privadas existentes en Ecuador que podrían aportar en un futuro proceso de implementación del nuevo dispositivo de identificación digital en el país.
Palabras-clave: DNIe, Identificación electrónica, gobierno electrónico, Ecuador.

ABSTRACT
At present, the need for a secure electronic identification device to identify y authenticate citizens in online activities is paramount, even more so in countries that are implementing e-government policies in their population y in the face of daily attacks Online spoofing. In this review article, an analysis is made of the security that exists in the implementation of the national electronic identification document (DNIe) in Spain, the versions that the device has had, the technology it currently has, the internal structure, The types of digital security certificates that the cryptographic chip stores, the public key infrastructure that supports its operation, y the proposed use cases for the device. Additional includes a review of countries that implement electronic identification devices in e-government environments for their citizens, the possible weaknesses presented in this type of cryptographic cards as well as the countermeasures defined by recognized authors in environments of lateral channel attacks, lastly A review of public y private institutions in Ecuador that could contribute to a future process of implementation of the new digital identification device in the country is presented.
KEYWORDS: DNIe; electronic identification; e-government; Ecuador

1. Introducción

Se vive uno de los tiempos más conflictivos en la lucha por mantener la privacidad en los datos, con cibercriminales acechando por doquier, haciendo uso de la tecnología para realizar análisis minuciosos de vulnerabilidades y encontrar fallos en dispositivos de seguridad calificados como seguros [1], en una sociedad en donde las personas se encuentran registradas en miles de bases de datos dispersas, haciendo uso de múltiples identidades en la red [2], existiendo inclusive restricciones mínimas e insuficiente protección a los menores de edad al momento de acceder a internet convirtiéndolos en entes vulnerables a actividades delictivas como abusos, pedofilia, suplantación de identidad, etc. [3]

La suplantación de identidad, el robo de datos y el acceso fraudulento en los sistemas de información ocurren con frecuencia, el objetivo de los atacantes es espiar y robar información confidencial de sus víctimas, así lo demuestra la empresa[4] la cual detectó un promedio de 45 diferentes ataques por segundo en América Latina en un periodo comprendido entre julio 2018 a julio 2019.

Por otra parte, [5] exponen que cuando existe una suplantación de identidad, es difícil poder distinguir al verdadero titular del impostor, y ésta suplantación, en el mayor de los casos es detectada después de haberse consumado un delito, cuando el titular de la información se encuentra involucrado en actos ilícitos o incluso cuando se ha tenido una afectación económica producto de transacciones electrónicas no autorizadas. Ya en el año 1987 [6] proponían las primeras debilidades al no usar tecnología de identificación digital, entre ellas: fotocopias de pasaportes por gobiernos discrepantes, números de tarjeta de crédito clonados y contraseñas vulnerables a hackers y grabaciones.

De la misma forma [7] coinciden en que uno de los retos generados por el rápido desarrollo de las tecnologías de la información es brindar y garantizar a los ciudadanos de mecanismos que aseguren la privacidad de su información. En el mismo sentido [8] señalan que es necesario implementar mecanismos de seguridad que permitan al común de los ciudadanos mantener su información personal íntegra, confidencial y segura, para con ésta confianza adquirida realizar transacciones electrónicas autorizadas y sentirse seguros que la información transmitida viaja por canales electrónicos confiables.

Para verificar la identidad de una persona y garantizar la privacidad en el acceso a los datos [9] exponen cuatros métodos distintos para hacerlo: conociendo una secuencia de seguridad (contraseña), portando un documento o carnet de identificación (medio físico), mediante la verificación de características propias del usuario (biometría) y por último verificando la posición geográfica de un usuario (georeferenciación). [5] concuerdan en que debe existir un equilibrio entre los mecanismos de seguridad para que, multiplicando los controles de acceso el fraude electrónico sea dificultoso y se minimice el acceso no autorizado a información privada, sin embargo partiendo de la premisa de que ningún sistema de seguridad es infalible, la recomendación sería entonces implementar sistemas de autenticación difíciles de violentar para que de esta manera el esfuerzo requerido en violentar el mismo sea superior a los beneficios obtenidos.

El mecanismo de seguridad que mayor expansión ha tenido hasta la actualidad es la contraseña, la cual se basa en el conocimiento que tiene un usuario sobre un conjunto de caracteres para autenticarse, y es debido a las vulnerabilidades y problemas generados en la implementación de autenticación por medio de contraseñas que surge la necesidad de implementar un segundo factor de autenticación utilizando por ejemplo un documento o carnet de identificación el cual permite autenticarse ante una persona o ante un dispositivo electrónico por medio de una serie de operaciones matemáticas tan complejas de forma que vulnerar la autenticación del usuario utilizando este segundo mecanismo sea una tarea realmente dificultosa [9].

Teniendo en cuenta que la validación de la identidad de una persona por medio de un carnet de identificación siempre se realizará de manera física, es preciso establecer procedimientos electrónicos para poder verificarla según los avances actuales de la tecnología. Es aquí donde surge el Documento Nacional de Identidad Electrónico (DNIe), el cual nace de la necesidad de otorgar identidad personal a los ciudadanos para acceder a servicios electrónicos acorde a los avances de la sociedad de la información (Ministerio del Interior - Gobierno de España, 2015).

Según lo indicado por [7][10], España es uno de los países pioneros a nivel mundial en la implementación de la tecnología del DNIe. En el Ecuador, tal como lo indica la Dirección General de Registro Civil, Identificación y Cedulación (2013), desde hace unos cinco años atrás se han desarrollado proyectos de

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 64-77 ISSN 2550-6730

actualización de la cédula de identidad, augurando la futura implementación de un estándar de identidad electrónica en el país, por lo cual el objetivo del presente estudio se centra en analizar la seguridad que brinda el dispositivo DNIe en los países donde se ha implementado, para de esta manera tener un punto de vista más amplio hacia su futura aplicación en el Ecuador, se detallan los usos propuestos por diferentes autores para el DNIe y una revisión de las instituciones que podrían aportar en un futuro proceso de implementación del dispositivo en el Ecuador.

2. Marco Teórico

DNIe

[10][11][12] exponen al DNIe como el documento que permite legitimar a su titular como auténtico y justifica de forma física y digital su identidad, así como la firma electrónica de documentos digitales, la unión de las medidas de acceso físico y las digitales ofrecen un nivel de protección alto permitiendo al usuario tener un dispositivo de autenticación prácticamente inviolable o falsificable. Este documento está formado sobre un soporte de policarbonato cuyo tiempo de duración se estima en 10 años como mínimo con un tamaño similar al de una tarjeta de crédito coincidiendo con lo indicado por [13] quien clasifica al DNIe como una tarjetas criptográficas dentro del grupo de tarjetas inteligentes, en la cual se pueden almacenar certificados digitales de seguridad de forma segura con la finalidad de firmar documentos o autenticarse sin necesidad que el certificado salga de la tarjeta gracias al uso del procesador criptográfico contenido en ella quien es el que realiza el proceso de la firma digital.

Versiones del DNIe

[10] indica que el DNIe en España se puso en marcha el 16 de marzo de 2006 siendo esta la primera versión del dispositivo en implementarse en dicho país. La versión vigente del DNIe en dicho país es la 3.0 la cual empezó a ser emitida a partir de enero del 2015. En dicha versión se incorpora la tecnología "Dual Interface" la cual permite conexión por medio de contactos o de forma inalámbrica mediante un emisor de frecuencia Near Field Communication (NFC). La interfaz con contactos permite mantener la compatibilidad del dispositivo con tecnologías anteriores, mientras que la conexión por radiofrecuencia permite leer el dispositivo mediante tecnología NFC (Ministerio del Interior - Gobierno de España, 2016). El objetivo de la versión 3.0 según lo explican [3] es facilitar su uso con teléfonos inteligentes evitando la limitante de acceso a lectores de tarjetas inteligentes por parte de los usuarios finales. En la figura 1 se detallan las características físicas del DNIe 3.0.

Near Field Communication (NFC)

[14] exponen que la tecnología de Comunicación de Campo Cercano por sus siglas en inglés NFC permite la conectividad entre dispositivos a una distancia máxima de 20 cm, la cual en la actualidad está siendo implementada por fabricantes de telefonía móvil y entidades bancarias para permitir al usuario final acceder a servicios electrónicos de una manera ágil y rápida.

Y es justamente mediante el estudio realizado por [15] en donde se propone la metodología utilizada para la autenticación mediante el DNIe a través de tecnología NFC, permitiendo el intercambio de información crucial por medio de comunicaciones inalámbricas seguras entre pares.

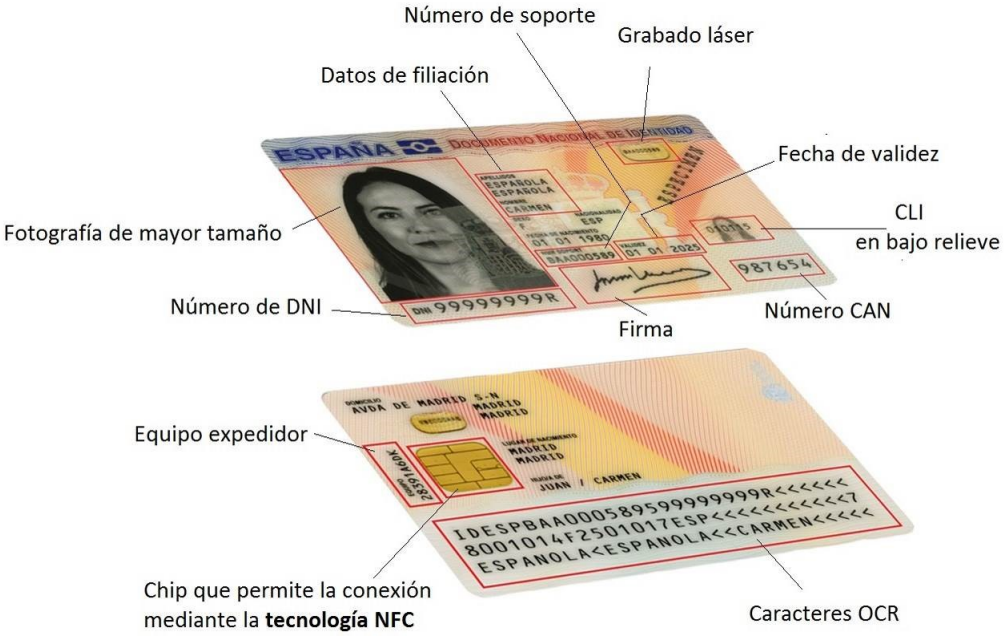

Figura 1: Descripción del DNI 3.0.
Fuente: (Ministerio del Interior - España, 2016)

Componentes y estructura interna del DNIe

El DNIe contiene los datos de filiación del ciudadano, la información biométrica (modelo dactilar, foto y firma manuscrita), y dos pares de claves RSA con sus correspondientes certificados de seguridad para autenticación y firma electrónica (Ministerio del Interior - Gobierno deEspaña, 2015). La información almacenada en el chip criptográfico se encuentra dividida en tres áreas con distintos niveles de acceso y condiciones de seguridad según lo descrito por [12][16][3]
Un área publica con acceso de solo lectura sin restricciones que contiene tres certificados x.509:

1. Certificado de seguridad único por cada DNIe el cual está asociado a la tarjeta inteligente con una clave pública RSA de 1024 bits.
2. Certificado de seguridad de la Autoridad de Certificación (CA), con una clave pública RSA de 1024 bits.
3. Certificado de la CA intermedia de la Dirección General de Policía, con una clave pública RSA de 2048 bits.

La segunda área del chip es privada con acceso de solo lectura posterior a la validación del código PIN del ciudadano (Personal Identification Number), esta sección contiene un certificado de seguridad para firma electrónica y un certificado de autenticación de usuario ambos una clave pública RSA de 2048 bits. La tercera área es de seguridad y con acceso de solo de lectura posterior a la verificación biométrica, esta acción solo es accesible desde los dispositivos biométricos ubicados en las oficinas de emisión de DNIe. Esta sección contiene los datos de filiación ciudadana (nombre, apellidos, fecha de nacimiento, etc.), una imagen digitalizada de la firma manuscrita del ciudadano y una fotografía del ciudadano.
De acuerdo a la estructura que posee el dispositivo de identificación electrónica antes descrito y por los niveles de seguridad establecidos en el chip, se desprende que detrás de la existencia del DNIe existe una

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 64-77 ISSN 2550-6730

infraestructura de clave pública (PKI) que soporta su funcionamiento y validación en España según lo descrito por [7].

Infraestructura de Clave Pública (PKI)

La PKI por sus siglas en inglés, tal como lo describe [7] es un conjunto de normas, procedimientos, software y personas, las cuales permiten la generación de certificados digitales de seguridad, mismos que tienen un tiempo de vigencia establecido de acuerdo a las normas legales de cada país y su funcionamiento se sustenta en la criptografía de clave pública desarrollada por [17], la PKI respalda el uso de la criptografía de clave pública según lo descrito por [18] puesto en este esquema la clave pública se almacena en un tercera entidad de confianza que valida la originalidad de la identidad del firmante.

El concepto de PKI, tal como indican [19] se ha afianzado a través de los últimos años usándose como referencia en la implementación de la nueva generación de aplicaciones haciendo posible el acceso a servicios de seguridad a gran escala inclusive en sistemas abiertos como la Internet.

La PKI según lo expone [20] forma parte del modelo de certificación TPT - Tercera Parte de Confianza o Trusted Third Party por sus siglas en inglés, la cual según lo indicado por [21] es el tercer nivel de seguridad en donde los fraudes de la autoridad de certificación deben ser detectables, en donde la autoridad de certificación no puede calcular las claves secretas de los usuarios y por medio de ésta entidad se puede comprobar la autenticidad de los certificados de seguridad electrónicos emitidos. Una PKI está formada por los siguientes componentes funcionales descritos por [13]: La Autoridad de Certificación (Certification Authority - CA), la autoridad de registro (Registration Authority - RA), la autoridad de Validación (Validation Authority - VA), la autoridad de sellado de tiempo (Time Stamping Authority - TSA). En la figura 2 se describe el modelo de referencia de la infraestructura de clave pública sobre la que funciona el DNIe en España en donde el proceso de pre personalización lo lleva a cabo la Fábrica Nacional de Moneda y Timbre y el proceso de expedición lo realiza el Ministerio del Interior mediante el organismo afiliado de la Dirección General de la Policía en calidad de Autoridad de Certificación Raíz.

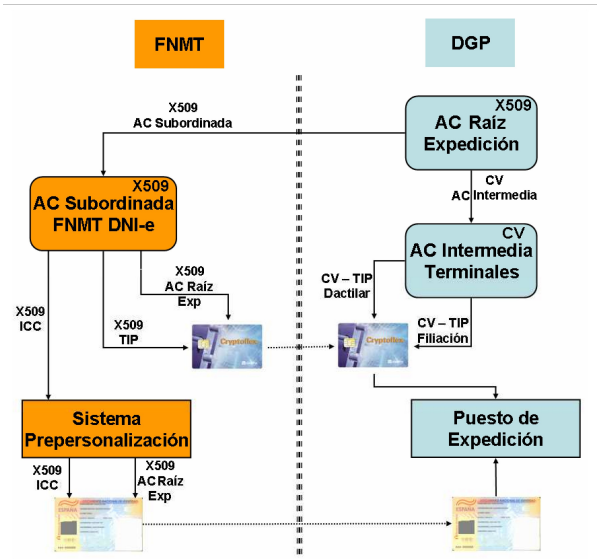

Figura 2: Modelo de referencia de proceso de pre personalización y expedición del DNIe
Fuente: (Crespo et al., 2006)

Los certificados digitales de seguridad que incorpora el DNIe cumplen con la función de confirmar que la clave criptográfica pública pertenece realmente a una persona determinada ayudando a evitar la suplantación de identidad, éstos certificados se componen de una clave pública, el nombre del titular, fecha de vencimiento, nombre de la autoridad de certificación, número de serie del certificado, y la firma digital del que otorga el certificado de seguridad según lo descrito por [22].

Las operaciones criptográficas de cifrado y descifrado que requieren el uso de una de las claves privadas almacenadas en el DNIe son ejecutadas por el chip interno, desempeñándose éste como una caja de seguridad digital para las claves privadas y como un coprocesador de operaciones criptográficas siempre y cuando se le suministre el PIN de usuario como método de autenticación [13].
Las áreas de uso del dispositivo DNIe incluyen transacciones comerciales, bancarias y servicios públicos. A continuación, se detallan algunos de ellos.
Usos del DNIe Las declaraciones de impuestos, el acceso a servicios de seguridad social, consulta de saldos de puntos de licencias de conducir, firma de contratos, registro de visitantes, transacciones financieras seguras en sistemas de administración público y privados son ejemplo de las áreas en donde se puede implementar el dispositivo ([11][13]).
En una investigación realizada por [23] se expone la futura utilización del DNIe como elemento para la autenticación de identidad del votante en un proceso de sufragio electrónico partiendo desde la autorización para realizar el voto hasta el proceso de la verificación individual de los resultados de la votación coincidiendo con lo propuesto por [24] quienes proponen la creación de una plataforma de sufragio seguro a través de Internet la cual permitiría recopilar firmas y soportar múltiples contextos mediante certificados digitales pudiendo ser utilizada dicha plataforma en votaciones de asambleas de accionistas, elección de dignidades populares, recolección de firmas de nominaciones, elecciones en reuniones de padres de familia en escuelas y colegios, entre las infinitas posibilidades de implementación del DNIe.
La posibilidad de implementar un sistema de control de transporte mediante GPS y autenticación vía DNIe para evitar vulnerabilidades relacionadas con suplantaciones de identidad en los conductores propuesta por [25], así como la metodología para autenticación en servicios de voz sobre IP mediante el dispositivo DNIe planteada por [26] son asimismo propuestas interesantes.
El sector de la salud también tiene un ejemplo de aplicación del DNIe mediante la propuesta de [27] en el cual presentan un caso real de éxito que permitió resolver incidentes relacionados con la privacidad de la información de los pacientes de un hospital en cumplimiento de la Ley Orgánica de Protección de Datos.
De forma adicional [3] presentan un uso muy particular del DNIe para realizar discriminaciones en cuanto a accesos de menores de edad en sitios web de adultos, es posible evitar suplantaciones de adultos haciéndose pasar como menores utilizando una validación de acceso a los sitios web mediante la fecha de nacimiento almacenada en el chip criptográfico del DNIe.
En el mismo sentido [28] realizaron una comparación entre el DNIe y una tarjeta inteligente para firmar prescripciones médicas, obteniéndose como resultado que el DNIe sobrepasa las funcionalidades de otras tarjetas de autenticación, pudiendo reemplazar a las mismas disminuyendo de esta forma los costos en la adquisición de dispositivos similares, unificando procesos y aprovechando la conectividad con tabletas y teléfonos inteligentes que el DNIe permite por medio de la tecnología NFC.
[29] proponen el uso del DNIe como testigo digital en procesos de evidencias electrónicas para escenarios de Internet de las cosas conectando el DNIe a través de una de sus interfaces (contactos o NFC) para firmar las evidencias directamente y obteniendo un código con validez legal asociado a la identidad del custodio de la evidencia facilitando su uso ante un tribunal de justicia sin tener que involucrar a terceras partes.
Con las demostraciones planteadas en las áreas antes mencionadas se visualiza que la implementación del DNIe genera un impulso en el aumento de transacciones comerciales electrónicas públicas y privadas haciendo que sea posible el desarrollo del gobierno electrónico (e-goverment) también denominado e-administración [10].
Gobierno electrónico [30] expresan que la interacción entre los ciudadanos con las administraciones gubernamentales a lo largo de los años ha sido una tarea compleja debido a las limitantes de horarios de oficina y largos tiempos de espera, coincidiendo con lo expuesto por [11] quienes plantean que el acceso a los servicios electrónicos debería estar disponible las 24 horas del día, siete días a la semana, eliminándose la dependencia del horario de atención de la administración pública hacia la ciudadanía, permitiendo la interacción entre autoridades, ciudadanos, empresas y otras autoridades [2].
La implementación de dispositivos de identificación electrónica hace posible la eliminación de la tediosa práctica de llenar formularios en las instituciones, disminuyendo la asistencia personal de los ciudadanos

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 64-77 ISSN 2550-6730

a las oficinas públicas [30], permitiendo obtener la información del ciudadano desde un sistema central de información gubernamental posibilitando realizar trámites electrónicos a distancia eliminando considerablemente los incomodos desplazamientos y las largas colas de espera, reduciendo así la pérdida de tiempo en que los ciudadanos se ven afectados [11].

Gobierno electrónico y la sociedad [7][31] coinciden en la necesidad de las instituciones gubernamentales en actualizar sus servicios en línea para que puedan adaptarse a la tecnología del DNIe, se debe implementar proyectos que acerquen la administración pública a la sociedad y permitan a sus ciudadanos disminuir los trámites burocráticos de acreditación de identidad para el acceso a los servicios electrónicos, de esta forma el proceso de renovación del documento de identificación obligará por si solo a que la población tenga mayor acceso al dispositivo.

El gobierno electrónico es por lo tanto el proceso de aplicación de las Tecnologías de la Información y Comunicaciones para facilitar los procedimientos administrativos, según lo indica [30]. Lo destacable del DNIe de acuerdo a lo descrito por [7] son las implicaciones sociales que genera y las facilidades a los ciudadanos para el acceso a servicios electrónicos a través de la incorporación de una identidad digital, concepto que surge por la disponibilidad y adopción de las tecnologías de Internet las cuales allanaron el camino hacia los métodos actuales de transacciones en línea [32].

De la misma forma [2] aseveran que el gobierno electrónico permite la interacción entre autoridades, ciudadanos, empresas y otras autoridades, en la misma línea [28] exponen que la protección de datos y la prevención del fraude en línea son aspectos de gran importancia en ambientes de eGovernment.

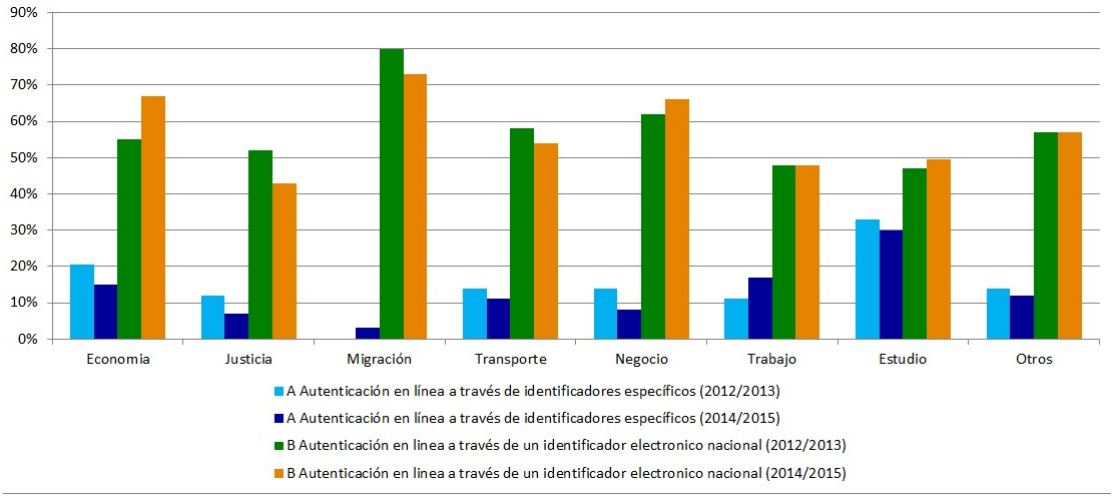

Figura 3: Uso de mecanismos de autenticación en 7 eventos de la vida (2012/2013 vs 2014/2015, EU28+, %)

Fuente: Adaptado de European Commission (2016)

En 2016 la European [33] estableció la necesidad de aumentar de manera más acelerada los servicios online en las administraciones públicas para satisfacer las expectativas de los ciudadanos y de las empresas, su informe proporciona información sobre el uso de medios de autenticación online. Se visualiza el aumento del uso del Identificador electrónico nacional para la autenticación de usuarios en siete eventos de la vida diaria de las personas en un periodo de análisis entre los años 2012 y 2015. En la figura 3 se detallan los resultados obtenidos.

Mientras que para el año 2018 la misma entidad confirmó que hubo un incremento del 34 % en la implementación de identificaciones electrónicas en los sitios web gubernamentales evaluados, de los cuales en el 18 % de estos se logró acceder a otro servicio sin necesidad de autenticarse nuevamente.

Países con dispositivos de identificación electrónica

Austria y Estonia son dos países referentes de Europa en términos de disponibilidad de gobierno electrónico, [30] indican que la mayor parte de los servicios de gobierno electrónico en Austria son accesibles a través de la web, mientras que Estonia lidera a nivel mundial la innovación de administración pública con una plataforma de voto electrónico online y una plan de residencia electrónica que incluye una tarjeta de identificación con chip, un lector de tarjetas y un generador de códigos con los cuales los residentes electrónicos pueden firmar documentos, identificarse y realizar trámites como por ejemplo la apertura de empresas en el país o el pago de impuestos sin necesidad de residir físicamente en el mismo [34].
Entre algunos ejemplos de implementaciones de soluciones de identidad electrónicas en Europa tenemos países como los referidos por [18] quien identificó a Finlandia como el primer país en emitir tarjetas electrónicas de identidad a sus ciudadanos en el año 1999 con el nombre de FinEID card, de la misma forma lo hizo Italia en el año 2001 implementando la CIE (Cartà d' Identita Elettronica), mientras que Bélgica empezó el plan piloto para emitir su EIC (Electronische Identiteitskaart) en el año 2003 según lo indicado por [35]. Australia también posee un documento de identidad similar denominado national document verification service (DVS) implementado a partir del año 2007 [36]
En Sudamérica Argentina es uno de los países que se encuentra migrando sus políticas de gobierno electrónico, un ejemplo de ello es que a partir del 1 de abril de 2017 el DNI digital será el único documento válido para autenticación en dicho país, teniendo un claro ejemplo de la transformación de la administración pública hacia la e-administración (Registro Nacional de las personas, 2017)
Es necesario señalar que el Ecuador se encuentra en un proceso de transformación de la administración pública hacia el gobierno electrónico, así lo demuestra la publicación de la [37] en donde se incluye al país en la segunda mejor categoría a nivel mundial con un alto nivel de participación electrónica sobre los servicios prestados por el gobierno coincidiendo con [38] quienes incluyen a Ecuador dentro de los países que están en proceso de transición hacia un nuevo sistema de identificación de próxima generación.
El Plan de Gobierno Electrónico en Ecuador de la Secretaria Nacional de la Administración Pública (2016) se incluye la organización del uso de certificados electrónicos y el desarrollo de la firma electrónica, existiendo tres instituciones vigentes calificadas para brindar servicios de certificación mediante infraestructura de clave pública como son el Banco Central del Ecuador, el Consejo de la Judicatura y la empresa privada Security Data. Cabe indicar que la empresa ANF Autoridad de Certificación Ecuador se encuentra en estado de liquidación [39]. En la figura 4 se muestra la estructura actual de la una de las entidades de certificación en Ecuador, el Consejo de la Judicatura:

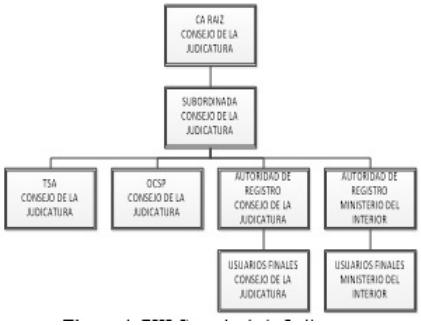

Figura 4: PKI Consejo de la Judicatura
Fuente: Adaptado de ARCOTEL (2016); Consejo de la Judicatura (2016)

Debilidades y amenazas del DNIe La conectividad de dispositivos móviles con el DNIe mediante tecnología NFC genera nuevos escenarios de amenazas, que no necesariamente dependen de la tecnología implementada en la tarjeta criptográfica, [40]confirmó la posibilidad de realizarse ataques de denegación de servicios a las infraestructuras PKI, por otra parte [41][42] propusieron una segunda forma de ataque mediante la instalación de aplicaciones ocultas en los dispositivos móviles (keylogger) la cual podría retransmitir información desde el dispositivo móvil de la víctima hacia otro destino (relay attack).

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 64-77 ISSN 2550-6730

[40] atribuía al factor humano como la mayor amenaza probable en un esquema de identificación electrónica, este error puede producirse al momento de enrolar el dispositivo por primera vez o al instante de tomar los datos biométricos para su registro en el chip.
Sin embargo, de acuerdo a las nuevas tendencias actuales en materia de investigación de criptoanálisis se confirma que la seguridad teórica implementada en las tarjetas criptográficas como el DNIe no garantiza su seguridad práctica debido a factores que no suelen ser tomados en cuenta al momento de diseñar el protocolo criptográfico esto a pesar de que según lo afirmado por [43] durante los últimos años se viene incrementando el uso de dispositivos electrónicos con características criptográficas para diversos fines (identificación personal, tarjetas de pago, etc.).
A los tipos de ataques cuyo objetivo es obtener información explotando las debilidades de los protocolos criptográficos de las tarjetas inteligentes se los denomina ataques de canal lateral (side cannel attacks) o por inducción de fallos (fault attacks), ejemplo de ello se tiene el conjunto de herramientas de software para ataques de canal lateral contra dispositivos criptográficos, en especial tarjetas inteligentes propuesto por [43].
De forma contraria, ante las eventuales debilidades presentadas en los sistemas criptográficos mediante la implementación de ataques de canal lateral, existen contramedidas que pueden ser aplicadas en diferentes niveles de abstracción de acuerdo a lo descrito por [44][45]

En el nivel físico: escudos, fuentes de alimentación desmontables para mejorar la resistencia de un dispositivo contra ataques físicos.
En el nivel tecnológico: CMOS alternativas para disminuir la dependencia de datos de consumo de energía.

En el nivel algorítmico: funciones de random, encriptación de buses, ocultación (utilizando retardos aleatorios, enmascaramiento de operaciones sensibles.

Para todos los niveles anteriores se puede incluso añadir ruido en amplitud como una solución genérica para disminuir la cantidad de información perdida por medio de canales laterales. De la misma forma existen las contramedidas en el nivel de protocolo, por ejemplo basadas en actualizaciones claves.

3. Conclusiones, Limitaciones y Trabajos Futuros

El dispositivo de identificación electrónica es un mecanismo de autenticación seguro considerado como un segundo factor de autenticación (algo que se sabe más algo que se tiene) el cual debe estar respaldado por una infraestructura de clave pública robusta para su correcta implementación. El dispositivo analizado es ideal para su aplicación en actividades electrónicas y comerciales en línea sin que existan restricciones de horarios, facilitando la prestación de servicios a los ciudadanos en ambientes de gobierno electrónico y generando confianza en las personas al saber que se posee una herramienta con la cual se evita el fraude y falsificación de identidades especialmente en Internet.
Ecuador posee una infraestructura de clave pública diversa, con instituciones gubernamentales y privadas que ofrecen servicios en el país, las cuales podrían aportar en conjunto en el proceso de la emisión de un nuevo documento de identificación electrónico acorde a las tendencias y estándares aplicados en otros países como el caso de la listas de servicios de confianza o Trusted Service List (TLS) en Europa.
Garantizar la accesibilidad a la información en un entorno de gobierno electrónico es un reto debido a la integración con tecnologías complejas como las tarjetas inteligentes, aun así, se avizora una importante implementación de dispositivos de identificación electrónica en áreas aún no tan difundidas como salud, justicia y voto electrónico, para lo cual es necesario que las instituciones públicas y privadas actualicen sus plataformas de servicios transaccionales online y de esta manera estar preparados ante una nueva herramienta de identificación nacional lo cual se traducirá en confianza por parte de los ciudadanos hacia

sus proveedores de servicios, el dispositivo permitirá entablar relaciones comerciales de gran nivel con cualquier parte del mundo teniendo los ciudadanos la seguridad que su identidad estará resguardada por una infraestructura robusta que deberá fortalecerse ante eventuales intentos de ataques electrónicos tan habituales hoy en día.

No se evidencia información oficial sobre la estructura interna de la actual cédula de identidad de Ecuador aunque en estudios referidos se establece que la misma incorpora características de almacenamiento de firma en fichas electrónicas, siendo ésta junto con el corto período de tiempo utilizado para la publicación las limitantes encontradas al momento de realizar una comparación cuantitativa con dispositivos de identificación electrónica implementados en otros países, por lo cual, para futuras investigaciones se propone realizar un análisis de laboratorio del documento de identificación vigente en Ecuador para definir la estructura del chip interno y las características que incorpora, adicional se recomienda realizar un estudio de las plataformas web en los distintos sectores de la administración pública para obtener un esquema actual de la gestión de gobierno electrónico con miras a su futura utilización.

Si bien es cierto, los sistemas criptográficos utilizados en la actualidad en los dispositivos de identificación electrónica como el caso del DNIe implementan tamaños grandes de claves que conllevan mucho esfuerzo invertido (tiempo y dinero) para poder descifrarlas y con los cuales se puede estar seguro por un buen tiempo, no es menos cierto que los actuales avances tecnológicos en materia de investigación de ataques de canales laterales se encuentra en aumento, por lo que habrá que estar atentos al constante avance tecnológico para establecer contramedidas en el momento en que se detecten debilidades y vulnerabilidades en los sistemas de cifrado actuales.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 64-77 ISSN 2550-6730

Referencias

[1] A. Corletti. "Seguridad en Redes". En: (2016).

[2] Flavio Corradini, Eleonora Paganelli y Alberto Polzonetti. "The e-Government digital credentials". En: *International Journal of Electronic Governance* 1.1 (2007), págs. 17-37.

[3] V. Gayoso Martínez, L. Hernández Encinas y A. Martín Muñoz. "La tarjeta de identidad española como método de autenticación en redes sociales". En: *VII Congreso Iberoamericano de Seguridad Informática*. 2013, págs. 32-44.

[4] Kaspersky. *Kaspersky registra 45 ataques por segundo en América Latina.* 2019. URL: `https://latam.kaspersky.com/blog/kaspersky-registra-45-ataques-por-segundo-en-america-latina/15274/`.

[5] Luis Gerardo Gabaldón y Wílmer Pereira. "Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico". En: *Sociologias* 20 (2008), págs. 164-190.

[6] Amos Fiat y Adi Shamir. "How to prove yourself: Practical solutions to identification and signature problems". En: *Conference on the theory and application of cryptographic techniques*. Springer, 1986, págs. 186-194.

[7] Javier Crespo Sánchez y col. "Hacia una nueva identificación electrónica del ciudadano: el DNI-e". En: (2006).

[8] Jordi Forne. "Criptografia y seguridad en comunicaciones". En: *Novática: Revista de la Asociación de Técnicos de Informática* 116 (1995), pág. 20.

[9] Simson Garfinkel, Gene Spafford y Mario Camou Riverol. *Seguridad y Comercio en el Web*. McGraw-Hill, 1999.

[10] Tomàs Baiget. "DNI electrónico (DNIe)". En: *Anuario ThinkEPI* 1 (2007), págs. 203-204.

[11] E. Directivos. "Características y funciones del DNI electrónico." En: (2008). URL: `http://search.ebscohost.com/login.aspx?direct=trueydb=fuayAN=40074735ylang=esysite=ehost-live`.

[12] Javier Espinosa-Garcia, L. Hernández Encinas y A. Queiruga Dios. "The new Spanish electronic identity card: DNI-e". En: *Conference on Cryptology and Digital Content Security*. 2007.

[13] R. Sarwat. "DNI-e Tecnología y Usos". En: *Móstoles, Madrid*. 64 (2010).

[14] Kevin Curran, Amanda Millar y Conor Mc Garvey. "Near Field Communication." En: *International Journal of Electrical & Computer Engineering (2088-8708)* 2.3 (2012).

[15] Jose Maria León-Coca y col. "Authentication systems using ID Cards over NFC links: the Spanish experience using DNIe". En: *Procedia Computer Science* 21 (2013), págs. 91-98.

[16] V. Gayoso Martínez y col. "A comparative study of three Spanish eGoverment smart cards". En: *Logic Journal of the IGPL* 25.1 (2017), págs. 42-53.

[17] Whitfield Diffie y Martin Hellman. "New directions in cryptography". En: *IEEE transactions on Information Theory* 22.6 (1976), págs. 644-654.

[18] Niklas Auerbach. "Anonymous digital identity in e-government". PhD Thesis. University of Zurich, 2004.

[19] Rolando Chaparro, Pablo Greenwood y Benjamín Barán. *Alternativa de Infraestructura de Clave Pública Basada en el uso de DNSSEC*. 2008.

[20] C. Adams. "Trusted Third Party. In H. C. A. van Tilborg y S. Jajodia (Eds.)" En: *Encyclopedia of Cryptography y Security* (), págs. 1335-1335.

[21] Marc Girault y Self-Certified Public Keys. "Advances in Cryptology-EUROCRYPT'91". En: *LNCS* 547 (1991), págs. 490-497.

[22] Gladys Stella Rodríguez. "La certificación electrónica venezolana: Desde una perspectiva reflexiva". En: *Revista de Derecho* 17.17 (2011).

[23] Emilia P. Belleboni y Justo Carracedo Gallardo. "Uso del DNIe para reforzar el anonimato en el voto telemático mediante tarjetas inteligentes". En: ().

[24] Rubén González Crespo y col. "Design of an Open Platform for Collective Voting through EDNI on the Internet". En: *E-Procurement Management for Successful Electronic Government Systems*. IGI Global, 2012, págs. 1-13.

[25] J. A. Gutierrez-de-Mesa y col. "The Cost of Development of a New System to Control Drivers using GPS location and Identification through the electronic ID card". En: (2009).

[26] Igor Ruiz-Agundez y Pablo G. Bringas. "Service authentication via electronic identification cards: voip service authentication through the DNIe". En: *2012 Annual SRII Global Conference*. IEEE, 2012, págs. 602-607.

[27] Luis Enrique Sanchez y col. "LOPD Compliance and ISO 27001 legal requirements in the Health Sector". En: *IEEE Latin America Transactions* 10.3 (2012), págs. 1824-1837.

[28] David Arroyo y col. "Using smart cards for authenticating in public services: A comparative study". En: *Advances in Intelligent Systems and Computing* (2015).

[29] Ana Nieto, Rodrigo Roman y Javier Lopez. "Testigo digital: delegación vinculante de evidencias electrónicas para escenarios iot". En: *II Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2016)* 6 (2016), pág. 2016.

[30] Clemens Orthacker y Thomas Zefferer. "Accessibility challenges in e-Government: an Austrian experience". En: *Proceedings of the Forth International Conference on Internet Technologies and Applications (ITA 2011)*. 2011, págs. 221-228.

[31] Pablo R. Prieto. "El DNI electrónico: ecosistema y uso en la e-administración local". En: *El profesional de la información* 20.3 (2011), pág. 277.

[32] J. L. Camp. "Digital identity". En: *IEEE Technology and society Magazine* 23.3 (2004), págs. 34-41.

[33] E. Commission. "eGovernment Benchmark 2016". En: 80 (2016). URL: `https://www.capgemini.com/resources/egovernment-benchmark-2016`.

[34] G. Estonia. "The digital society." En: (2016). URL: `https://e-estonia.com/e-residents/about/`.

[35] Alea Fairchild. "The Evolution of the e-ID card in Belgium: data privacy and multi-application usage". En: *Sixth International Conference on Digital Society*. 2012.

[36] Organisation for Economic Co-operation y Development. *National strategies and policies for digital identity management in OECD countries*. OECD Publishing, 2011.

[37] ONU. "United Nations e-goverment survey 2016." En: *New York: Department of Economic and Social Affairs* (2016). URL: `http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf`.

[38] ITU. *Review of National Identity Programs*. 2016. URL: `https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/Review%20of%20National%20Identity%20Programs.pdf`.

[39] Arcotel. "Registro Publico de Entidades de Certificacion y Terceros Vinculados." En: (2016). URL: `http://www.arcotel.gob.ec/entidades-de-certificacion-firma-electronica/`.

[40] Siddhartha Arora. "National e-ID card schemes: A European overview". En: *Information Security Technical Report* 13.2 (2008), págs. 46-53.

[41] Julio José Píñar Figueroa y José Camacho Páez. "Pago móvil mediante NFC: Estudio y modelo de vulnerabilidad". En: (2016).

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 64-77 ISSN 2550-6730

[42] Michael Roland, Josef Langer y Josef Scharinger. "Practical attack scenarios on secure element-enabled mobile devices". En: *2012 4th International Workshop on Near Field Communication*. IEEE, 2012, págs. 19-24.

[43] Alberto Fuentes y col. "Design of a Set of Software Tools for Side-Channel Attacks". En: *IEEE Latin America Transactions* 13.6 (2015), págs. 1966-1978.

[44] Stefan Mangard, Elisabeth Oswald y Thomas Popp. *Power analysis attacks: Revealing the secrets of smart cards*. Vol. 31. Springer Science & Business Media, 2007.

[45] François-Xavier Standaert. "Introduction to side-channel attacks". En: *Secure Integrated Circuits and Systems*. Springer, 2010, págs. 27-42.